Draft for Industry Consultation

The Central Bank of The Bahamas

GUIDELINES ON THE PREVENTION & DETECTION OF MONEY LAUNDERING FOR LICENSEES

The Central Bank of The Bahamas
The Bank Supervision Department
Frederick Street
Nassau, Bahamas

Telephone: 242-302-2615
Facsimile: 242-356-3909

TABLE OF CONTENTS

APPENDICES **PAGES**

SCOPE

The Central Bank of The Bahamas ("the Central Bank") is responsible for the licensing, regulation and supervision of banks and trust companies ("licensees") operating in and from within The Bahamas pursuant to The Banks and Trust Companies Regulation Act, 2000 ("BTCRA"), and The Central Bank of The Bahamas Act, 2000 ("CBBA"). Additionally, the Central Bank has the duty, in collaboration with financial institutions, to promote and maintain high standards of conduct and management in the provision of banking and trust services.

All licensees are expected to adhere to the Central Bank's licensing and prudential requirements and ongoing supervisory programmes, including periodic onsite examinations, and required regulatory reporting. Licensees are also expected to conduct their affairs in conformity with all other Bahamian legal requirements.

The BTCRA directs the Inspector of Banks and Trust companies ("the Inspector") to ensure that Licensees have in place strict Know-Your-Customer ("KYC") rules that promote high ethical and professional standards, and so prevent the use of the Licensees for criminal purposes. The Inspector is required to ensure effective offsite supervision of licensees and is empowered to conduct onsite examinations for the purpose of satisfying himself that the provisions of *inter alia* the Financial Transactions Reporting Act, 2000 ("FTRA") and the Regulations made thereunder are being complied with.

These Guidelines incorporate both the mandatory minimum requirements of the Financial Transactions Reporting Regulations, 2000 ("FTRR") and industry best practices. It is, therefore, expected that all Licensees of the Central Bank pay due regard to these Guidelines in developing responsible anti-money laundering ("AML") procedures suitable to their business. If a Licensee appears not to be doing so the Central Bank will seek an explanation and may conclude that the Licensee is carrying on business in a manner that may give rise to sanctions under the applicable legislation.

It is important that the management of every Licensee view money laundering prevention as part of their risk management strategies and not simply as a stand-alone requirement that is being imposed by the legislation. Money laundering prevention should not be viewed in isolation from a Licensee's other business systems and needs.

These Guidelines have been prepared in consultation with those financial institutions and industry organisations that expressed an interest in being consulted in the course of the development of these Guidelines. The scope of these Guidelines covers all mainstream fiduciary, banking, lending and deposit taking activities of Central Bank Licensees.

However, where a Licensee is a part of an international group, it is recommended that a group policy be followed to the extent that all overseas branches, subsidiaries and associates where control can be exercised, ensure that verification of identity and record keeping practices are undertaken at least to the standards required under Bahamian law or, if standards in the host country are considered or deemed more rigorous, to those higher standards. Reporting procedures and the offences to which the money laundering legislation in The Bahamas relates must be adhered to in accordance with Bahamian laws and practices.

These Guidelines replace the existing Guidelines on Anti-Money Laundering and Suspicious Transactions Reporting for Banks and Trust Companies issued by the Financial Intelligence Unit ("FIU") in 2001, but only in relation to anti-money laundering and know your customer procedures. Licensees should continue to adhere to the FIU's Guidelines insofar as they relate to suspicious transactions reporting.

Where Licensees observe unusual activity in relation to any client account they should question the customer concerned, even if this means asking "awkward" questions. Any failure by the customer to provide credible answers will almost always give grounds for further enquiry about his activities, make the Licensee reconsider the wisdom of doing business with him and, potentially, lead to a suspicious transaction report ("STR") being made.

There is a risk that efforts to detect money laundering and to trace the assets will be impeded by the use of alternative undetected channels for the flow of illegal funds consequent on an automatic cessation of business (because a Licensee suspected that funds stemmed from illegal activity). To avoid that risk, Licensees should report their suspicions to the FIU and seek permission from the FIU to continue the business relationship or transaction. In carrying out transactions where a Licensee is considering making a STR, the Licensee should consider duties owed to third parties such as in the case of a constructive trustee. In such cases, it is recommended that independent legal advice is sought.

Consistent with the requirements of the law these Guidelines cover:-

- Internal controls, policies and procedures (Section III]
- Risk Rating Customers (Section IV);
- Verification of Customer Identity (Section V);
- Record Keeping (Section VI);
- The role of the Money Laundering Reporting Officer ("MLRO") (Section VII); and,
- Education and training of employees in the procedures, laws and detection of suspicious transactions (Section VIII).

I - BACKGROUND

1 The Bahamian law relating to money laundering is contained in the Proceeds of Crime Act, 2000 ("POCA"), the FTRA, the FTRR , the Financial Intelligence Unit Act, 2000 and the Financial Intelligence (Transactions Reporting) Regulations, 2001. This legislation is summarized in Appendix A.

What Is Money Laundering?

2 Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. If undertaken successfully, it also allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of income (see sections 40, 41 and 42 of the POCA).

The Need To Combat Money Laundering

3 In recent years there has been a growing recognition that it is essential to the fight against crime that criminals be prevented, whenever possible, from legitimizing the proceeds of their criminal activities by converting funds from "dirty" to "clean".

4 The ability to launder the proceeds of criminal activity through the financial system is vital to the success of criminal operations. Those involved need to exploit the facilities of the world's financial institutions if they are to benefit from the proceeds of their activities. The increased integration of the world's financial systems, and the removal of barriers to the free movement of capital, has enhanced the ease with which proceeds of crime can be laundered and have complicated the tracing process.

5 Thus, The Bahamas, as a leading financial centre, has an important role to play in combating money laundering. Financial institutions that knowingly become involved in money laundering risk prosecution, the loss of their good reputation and the loss of their entitlement to operate in or from within The Bahamas.

Stages of Money Laundering

6 There is no one single method of laundering money. Methods can range

from the purchase and resale of a luxury item (e.g., cars or jewelry) to passing money through a complex international web of legitimate businesses and "shell" companies. Initially, however, in the case of drug trafficking and other serious crimes enforceable under the POCA, the proceeds usually take the form of cash which needs to enter the financial system by some means.

7 Despite the variety of methods employed, the laundering process is accomplished in three stages, which may comprise numerous transactions by the launderers that could alert a financial institution to criminal activity:

a) Placement - the physical disposal of cash proceeds derived from illegal activity;

b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity; and,

c) Integration – the attempt to legitimize wealth derived from criminal activity. If the layering process has been succeessful, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

8 The three basic stages may occur as separate and distinct phases. They may occur simultaneously or, more commonly, they may overlap. How the stages are used depends on the available laundering mechanisms and the requirements of the criminal organisations.

9 Certain points of vulnerability have been identified in the laundering process which the money launderer finds difficult to avoid and where the activities are therefore more susceptible to being recognised, namely:

- entry of cash into the financial system;
- cross-border flows of cash; and,
- transfers within and from the financial system.

Vulnerability Of Banks And Trust Companies To Money Laundering

10 Efforts to combat money laundering largely focus on those points in the

process where the launderer's activities are more susceptible to recognition and have, therefore, to a large extent concentrated on the deposit taking procedures of financial institutions, i.e., the placement stage. However, it is emphasised that there are many crimes where cash is not involved. Financial institutions should consider the money laundering risks posed by the products and services they offer, particularly where there is no face-to-face contact with the customer, and devise their procedures with due regard to that risk.

11 The most common form of money laundering that financial institutions will encounter on a day to day basis, in respect of their mainstream banking business, takes the form of accumulated cash transactions which will be deposited in the banking system or exchanged for value. Electronic funds transfer systems increase the vulnerability by enabling the cash deposits to be switched rapidly between accounts in different names and different jurisdictions.

12 In addition, financial institutions as providers of a wide range of services are vulnerable to being used in the layering and integration stages of money laundering. Mortgage and other loan accounts may be used as part of this process to create complex layers of transactions.

II - WHAT THE BAHAMIAN LAW REQUIRES

The Bahamian Law – Outline of the legislation

13 The Bahamian law relating to money laundering is contained in the following legislation:

- The Proceeds of Crime Act, 2000;
- The Financial Transactions Reporting Act, 2000 ;
- The Financial Transactions Reporting (Amendment) Act, 2001;
- The Financial Transactions Reporting (Amendment) Act, 2003;
- The Financial Transactions Reporting Regulations, 2000;
- The Financial Transactions Reporting [Amendment] Regulations, 2001;
- The Financial Transaction Reporting (Amendment) Regulations, 2003
- The Financial Intelligence Unit Act, 2000
- The Financial Intelligence Unit (Amendment) Act, 2001; and
- The Financial Intelligence (Transactions Reporting) Regulations, 2001

THE PROCEEDS OF CRIME ACT, 2000

14 The POCA criminalizes money laundering related to the proceeds of drug trafficking and other serious crimes. The POCA also provides for the confiscation of the proceeds of drug trafficking or any relevant offence as described in the Schedule to the Act; the enforcement of confiscation orders and investigations into drug trafficking, ancillary offences related to drug trafficking and all other relevant offences.

The law requires financial institutions to inform the FIU or an authorized Police officer of any suspicious transactions. The POCA provides immunity to such persons from legal action by clients aggrieved by the breach of confidentiality. It should be noted that the reporting of suspicious transactions is mandatory and a person who fails to report a

suspicious transaction is liable to prosecution.

THE FINANCIAL TRANSACTIONS REPORTING ACT, 2000

15 The FTRA imposes mandatory obligations on financial institutions to: verify the identity of existing and prospective facility holders and persons engaging in occasional transactions; to maintain verification and transaction records for prescribed periods; and to report suspicious transactions, which involve the proceeds of criminal conduct as defined by the POCA, to the FIU.

The Financial Transactions Reporting (Amendment) Act, 2003

16 The Financial Transactions Reporting (Amendment) Act, 2003, *inter alia*, requires financial institutions to verify the identity of facility holders who have facilities which were established prior to 29th December 2000 ("an existing facility holder"). In addition to the existing obligation to verify the identity of any facility holder, the Amending Act requires that financial institutions must also verify the identity of on any person (whether as a facility holder or not) whom they know, suspect or have reasonable grounds to suspect is conducting or proposes to conduct a transaction which involves the proceeds of criminal conduct as defined in the POCA or is an attempt to avoid the enforcement of the POCA. Verification should take place as soon as practicable after the financial institution has the relevant knowledge or suspicion.

THE FINANCIAL TRANSACTIONS REPORTING REGULATIONS, 2000 ("FTRR")

17 The FTRR, *inter alia*, sets out the evidence that financial institutions should obtain in satisfaction of any obligation to verify the identity of a facility holder.

THE FINANCIAL TRANSACTIONS REPORTING [AMENDMENT] REGULATIONS, 2003

18 The Financial Transactions Reporting (Amendment) Regulations, 2003 *inter alia*, introduces a new regulation 3 which sets out the minimum information that financial institutions must obtain when they seek to

verify the identity of individual customers. In addition, the new regulation 3 introduces a risk based approach to customer due diligence and provides financial institutions with guidance on the type of information and documentation they may rely upon (apart from the required information) when verifying an individual customer's identity.

The Financial Intelligence Unit Act, 2000 ("FIUA")

19 The Financial Intelligence Unit Act, 2000 establishes the FIU, which has power, *inter alia*, to obtain, receive, analyse and disseminate information, which relates to or may relate to offences under the POCA.

The Financial Intelligence (Transactions Reporting) Regulations, 2001 ("FITRR")

20 The Financial Intelligence (Transactions Reporting) Regulations, 2001 require financial institutions to establish and maintain identification, record-keeping, and internal reporting procedures, including the appointment of an MLRO. These Regulations also require financial institutions to provide appropriate training for relevant employees to make them aware of the statutory provisions relating to money laundering.

Outline of Money Laundering Offences, Defences And Penalties

21 Concealing, Transferring Or Dealing With The Proceeds Of Criminal Conduct

It is an offence to use, transfer, send or deliver to any person or place, or to dispose of, convert, alter or otherwise deal with any property, for the purpose of concealing or disguising such property, knowing, suspecting or having a reasonable suspicion that the property (in whole or in part, directly or indirectly) is the proceeds of criminal conduct. This offence is found in section 40 of the POCA.

22 Assisting Another To Obtain, Conceal, Retain Or Invest The Proceeds Of Criminal Conduct

It is an offence for any person to provide assistance to another for the purpose of obtaining, concealing, retaining or investing funds. For a person to be convicted of this offence, he must know or suspect that the other person is someone who is or has been engaged in criminal conduct or has benefited from criminal conduct. This offence is found in section 41 of the POCA.

It is a defence to prove that a person did not know, suspect or have reasonable grounds to suspect that the funds in question are the proceeds of criminal conduct, or that he intended to disclose to a police officer his suspicion, belief or any matter on which such suspicion or belief is based, but there was a reasonable excuse for his failure to make any such disclosure.

23 Acquisition, Possession or Use

It is an offence to acquire, use or possess property which are the proceeds (whether wholly or partially, directly or indirectly) of criminal conduct, knowing, suspecting or having reasonable grounds to suspect that such property are the proceeds of criminal conduct. Having possession is construed to include doing any act in relation to the property. This offence is found in section 42 of the POCA.

It is a defence that the person charged acquired or used the property in question or had possession of it for adequate consideration. [NB: The provision for any person of goods or services which assist in the criminal conduct does not qualify as consideration for the purposes of this offence.]

24 Failure to Disclose

It is an offence for a person to fail to disclose to the police or the FIU his knowledge or suspicion that another person is engaged in money laundering, as soon as reasonably practicable after the knowledge or suspicion comes to his attention in the course of his trade, profession, business or employment. The offence of failing to report the knowledge, suspicion or reasonable suspicion of money laundering is found in section 43(2) of the POCA,

The FTRA makes it an offence, in section 14, for financial institutions to

fail to disclose to the FIU any transaction which a customer has sought to conduct by through or with the institution, where the institution knows, suspects or has reasonable grounds to suspect that the transaction involves the proceeds of criminal conduct, as soon as practicable after forming that suspicion.

The STR should be made in writing containing the necessary information in accordance with the FTRA. However, where the urgency of the situation requires it, the STR may be made orally to the FIU. As soon as possible thereafter, a report that complies with the provisions of the FTRA should be forwarded to the FIU.

It is a defence to prove that the defendant took all reasonable steps to ensure that he complied with the statutory requirement to report a transaction or proposed transaction; or that in the circumstances of the particular case he could not reasonably have been expected to comply with the provision. In the case of a person who is employed by a financial institution, internal reporting in accordance with the procedures laid down by the employer, pursuant to the Financial Intelligence (Transactions Reporting) Regulations, 2001, will satisfy the requirement to report suspicious transactions. The FTRA and The Financial Intelligence Unit Act, 2000 protects those financial institutions reporting suspicions of money laundering from claims in respect of any alleged breach of client confidentiality.

25 **Tipping Off**

It is also an offence both under section 44 of the POCA and section 20(4) of the FTRA to tip off the subject of a money laundering investigation, or a third party, about an investigation or proposed investigation into money laundering, or that an STR has been made or that the making of such a report is contemplated**,** or any matter which is likely to prejudice such an investigation.

Preliminary enquiries of a customer in order to verify his identity or to ascertain the source of funds or the precise nature of the transaction being undertaken will not trigger a tipping off offence before an STR has been submitted in respect of that customer unless the enquirer knows that an investigation is underway or the enquiries are likely to prejudice an investigation. Where it is known or suspected that an STR has already been filed with the FIU, the Police or other authorised agency and

it becomes necessary to make further enquiries, great care should be taken to ensure that customers do not become aware that their names have been brought to the attention of the authorities.

It is a defence under the POCA if the person making the disclosure proves he did not know or suspect that the disclosure was likely to prejudice the investigation, or that the disclosure was made under a lawful authority or with reasonable excuse.

Under the FTRA it shall be a defence if the person making the disclosure proves that he took all reasonable steps to ensure that he complied with the provisions of the FTRA, or could not reasonably have been expected to comply.

26 Constructive Trust

The duty to report suspicious transactions and to avoid "tipping off" leads to a conflict between the reporting Licensee's responsibility under the criminal law and its obligation, as a constructive trustee, to a victim of fraud and other crimes under the civil law.

A financial Licensee's liability as a constructive trustee arises when it becomes suspicious that the funds in a customer's account rightfully belong to a third party. The financial Licensee then takes on the obligation of constructive trustee for the rightful owner. If the funds are paid away other than to the rightful owner, the civil law treats the Licensee as though it were a trustee for the funds, and holds the Licensee liable to make good the loss suffered. Having a suspicion which it considers necessary to report under the money laundering legislation may, prima facie, indicate that it knows or should know that the funds belong to a third party.

Given the absolute nature of the prohibition in the criminal law, if a Licensee makes a disclosure under the money laundering legislation, and is acting in accordance with the FIU or the investigating officer's consent in paying out the money, the risk of the Licensee being held liable by a civil court as constructive trustee is considered to be slight.[1]

However, to minimise the liability, the following procedures should be followed

[i] When evaluating a suspicious transaction, the MLRO should consider whether there is a constructive trust issue involved. If the MLRO concludes that there is reason to believe that the Licensee may incur a liability as a constructive trustee, the precise reasons for this belief should be reported to the FIU immediately, along with the other matters giving rise to suspicion that the funds relate to the proceeds of crime. The constructive trust aspects should be set out clearly in the report. Neither the customer nor any third party should be tipped off.

[ii] On receipt of the report, the FIU will evaluate the information and "fast track" the report to the appropriate investigator who will determine whether the "consent" to undertake the transaction can be issued.

[iii] Where a suspicious transaction report has previously been made to the FIU, and a potential constructive trust issue comes to light subsequently, the FIU (or the designated investigator) should be provided with an immediate further report indicating the reasons why a constructive trust situation is believed to have arisen.

27 **Penalties**

Tipping off under the POCA carries a maximum penalty of ten years imprisonment or an unlimited fine or both.

Under the FTRA tipping off carries a maximum penalty on summary conviction of two years imprisonment.

Failure to disclose knowledge or suspicion of money laundering carries a maximum penalty of ten years imprisonment and/or an unlimited fine under the POCA. The penalty under the FTRA on summary conviction is a maximum fine of $20,000.00 (in the case of an individual) or $100,000.00 (in the case of a body corporate).

The other offences carry a maximum penalty of twenty years imprisonment and/or an unlimited fine.

(See a summary of the legislation in Appendix A of these Guidelines.)

28 **Verification**

Every financial institution commits an offence when it:

(i) fails to verify the identity of an existing facility holder;

(ii) fails to verify the identity of a new customer before permitting such customer to become a facility holder;

(iii) permits a facility holder to conduct an occasional transaction through that financial institution, without first having verified the identity of that facility holder, where the amount of cash involved in the transaction exceeds $15,000.00;

(iv) permits a facility holder to conduct an occasional transaction through that financial institution, without first having verified the identity of that facility holder, where the amount of cash involved in the transaction exceeds $15,000.00 and it appears to that financial institution that the person conducting the transaction is doing so on behalf of any other person or persons; and,

(v) fails to verify the identity of a facility holder whenever it appears that two or more (occasional) transactions are or have been deliberately structured to avoid lawful verification procedures in respect of the person(s) conducting the transaction(s) and the aggregate amount of cash involved in the transaction(s) exceed $15,000. Verification should be conducted as soon as practicable after the financial institution becomes aware of the foregoing circumstances.

Defence: It is a defence to a charge against a person if he proves that he took all reasonable steps to ensure that he complied with these provisions, or could not reasonably have been expected to comply in the circumstances of the particular case.

Penalty: On summary conviction the penalty for an individual is a fine not exceeding $20,000.00; in the case of a body corporate the penalty is a fine not exceeding $100,000.00.

29 **Retention of Records**

Every financial institution commits an offence if it fails, without reasonable excuse, to retain or to properly keep records sufficient to satisfy the requirements of the FTRA.

Penalty: On summary conviction the penalty for an individual is a fine not exceeding $20,000.00; in the case of a body corporate the penalty is a fine not exceeding $100,000.00.

30 **Interpretation**

In these Guidelines, unless the context otherwise requires:

[a] The term "criminal conduct" includes -

(1) drug trafficking;

(2) bribery and corruption;

(3) money-laundering;

(4) any offence which may be tried in the Supreme Court of The Bahamas other than a drug trafficking offence; and,

(5) an offence committed anywhere that, if committed in The Bahamas, would constitute an offence in The Bahamas as set out in the Schedule to the POCA.

[b] "facility" means any account or arrangement which is provided by a financial institution to a facility holder which may be used by the facility holder to conduct two or more transactions. It specifically includes provision for facilities for safe custody, including safety deposit boxes;

[c] a "facility holder" is the person in whose name the facility is established and includes any person to whom that facility is assigned or who is authorised to conduct transactions through that facility;

[d] an "occasional transaction" is a cash transaction that involves a payment, deposit, withdrawal, debit, repayment, encashment, exchange, or transfer of cash that is conducted by any person otherwise than through a facility of which that person is a facility holder; and

[e] a provision of a statute or regulation is, unless otherwise indicated, deemed to include a reference to such provision as amended, modified or re-enacted from time to time.

Any other terms used throughout this document not defined herein may

be found in the relevant legislation.

Responsibilities of the Central Bank

31 The fact that deposit-taking institutions are particularly vulnerable to use by money launderers means that the Central Bank maintains a keen interest in measures aimed at countering money laundering.

The Central Bank has informed all of its Licensees that failure to install or maintain adequate policies and procedures relating to money laundering would be taken into account in determining if the licensee continues to satisfy the criteria for licensing laid down in the BTCRA. Further, it has advised all licensees that these Guidelines would be used as part of the criteria against which it will assess the adequacy of a Licensee's systems to counter money laundering. With the exception of those instances where a Licensee has been examined by the Central Bank, Licensees are required to instruct their external auditors to prepare and submit a report during the course of the annual audit of financial statements on the adequacy of policies and procedures relating to AML specified in the FTRR. A copy of such report must be forwarded to the Central Bank within four months of the end of the financial year.

The POCA requires the supervisory authorities of financial institutions themselves to report any information they obtain which in their opinion indicates that any person has or may have been engaged in money laundering and to disclose that information to the FIU or the law enforcement authorities.

III - INTERNAL CONTROLS, POLICIES AND PROCEDURES

32 Licensees are required to establish clear responsibilities and accountabilities to ensure that policies, procedures, and controls which deter criminals from using their facilities for money laundering, are implemented and maintained, thus ensuring that they comply with their obligations under the law.

33 All Licensees are required to establish a point of contact with the FIU in order to handle the reported suspicions of their staff regarding money laundering. Such institutions are required to appoint an MLRO to undertake this role, and such officer is required to be registered with the FIU. Financial institutions are also required to appoint a Compliance Officer ("CO") who shall ensure full compliance with the laws of The Bahamas (see regulation 5 of the Financial Intelligence (Transactions Reporting) Regulations, 2001).

34 All Licensees are required to:

(i) introduce procedures for the prompt investigation of suspicions and subsequent reporting to the FIU;

(ii) provide the MLRO with the necessary access to systems and records to fulfill this requirement;

(iii) establish close co-operation and liaise with the Central Bank ;

(iv) notify the Central Bank of the name(s) of the MLRO and the CO;

(v) include in the notification a statement that the MLRO and the CO are fit and proper persons, and

(vi) notify the Central Bank where there are any changes to the MLRO and the CO.

35 A Licensee may choose to combine the roles of the CO and the MLRO depending upon the scale and nature of business. The roles might be assigned to its Inspection, Fraud or Compliance Department.

36 The legislation places an obligation on all financial institutions from time to time to ensure compliance with policies, procedures, and controls relating to money laundering activities to satisfy the requirements of the FTRR and the Financial Intelligence (Transactions Reporting) Regulations, 2001. Larger Licensees may wish to assign this role to their

Internal Audit or Compliance Departments. Smaller Licensees may wish to introduce a regular review by management.

IV - RISK RATING CUSTOMERS

International Standards

37 In its paper issued in October, 2001 on Customer Due Diligence for Banks, The Basel Committee on Banking Supervision recognised that adequate KYC policies and procedures have particular relevance to the safety and soundness of banks, in that such policies:

(i) prevent reputation risk and preserve the integrity of the banking system by preventing the use of the bank for criminal purposes; and,

(ii) complement the risk management strategy of banks (by enabling them to identify, limit and control risk exposure in assets and liabilities).

Similarly, the Financial Action Task Force ("FATF"), in its revised 40 Recommendations on Anti-Money Laundering and Combating the Financing of Terrorism, issued in June 2003, also recommends that financial institutions adopt a risk based approach to customer due diligence.

The FTRA and FTRR, adopt the risk based approach recommended by the Basel Committee and the FATF. The FTRR gives financial institutions the discretion to determine the appropriate level of information and documentation required to verify customer identity based on the nature and degree of risk inherent in the customer relationship. This approach is in keeping with international best practices.

Developing a Risk Rating Framework

38 Every Licensee is required to develop and implement a risk rating framework which is approved by its Board of Directors as being appropriate for the type of products offered by the Licensee, and capable of assessing the level of potential risk each client relationship poses to the Licensee. As part of the on-going onsite examination program, Central Bank onsite examiners will assess the adequacy of Licensees' risk rating policies, processes and procedures, in light of the type of business conducted by Licensees, as well as the extent to which Licensees have adhered to legislative requirements.

As a minimum the risk rating framework should include:

(i). Differentiation of client relationships by risk categories (such as high, moderate or low);

(ii) Differentiation of client relationships by risk factors (such as products, client type/profession, country of domicile, complexity of ownership and legal structure, source of business, type of assets, size and volume of transactions, type of transactions, cash transactions, adherence to client activity profile);

(iii)The KYC documentation and due diligence information requirements appropriate for each Risk Category and Risk Factor; and,

(iv) A process for the approval of the downgrading/upgrading of risk ratings.

The risk rating framework should provide for the periodic review of the customer relationship to allow the Licensee to determine whether any adjustment should be made to the risk rating. The review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

39 The risk rating framework should include customer acceptance and on-going monitoring policies and procedures that assist the Licensee in identifying the types of customer that are likely to pose a higher than average risk of money laundering. A more extensive customer due diligence process should be adopted for higher risk customers. There should also be clear internal guidelines on which level of management is able to approve a business relationship with such customers. The risk rating framework should provide for documentation of any changes in a customer's risk rating and the reason(s) for such change. In determining the risk profile of any customer, licensees should take into account factors such as the following risk criteria (which are not set out in any particular order of importance nor should they be considered exhaustive):

(i) geographical origin of the customer;

(ii) geographical sphere of customer's business activities including the the location of the counterparties with which the customer conducts transactions and does business, and whether the customer is otherwise connected with certain high risk jurisdictions, or those known to the licensee to lack proper standards in the prevention of money laundering or customer due diligence process;

(iii) nature of the customer's business, which may be particularly susceptible to money laundering risk, such as casinos that handle large amounts of cash;

(iv) nature of activity;

(v) frequency of activity;

(vi) customer type, e.g. potentates/politically exposed persons ("PEPs");

(vii) type, value and complexity of the facility;

(viii) unwillingness of the customer to cooperate with the licensee's customer due diligence process for no apparent reason;

(ix) unreasonable pattern of account activity given the Licensee's information on the customer;

(x) for a corporate customer, unduly complex structure of ownership for no apparent reason;

(xi) whether there is any form of delegated authority in place (e.g.: power of attorney);

(xii) whether hold mail arrangements are in place;

(xiii) whether an account/business relationship is dormant; and,

(xiv) any other information that raises suspicion of the customer being connected to money laundering.

40 **Prospective Customers**

Licensees should assess the potential risk inherent in each new client relationship prior to establishing a business relationship. This assessment should take account of whether and to what extent a customer may expose the Licensee to risk, and of the product or facility to be used by the customer. Based on this assessment, the Licensee should decide whether or not to establish a facility for the customer concerned or to continue with it.

41 **Existing Customers**

Licensees are required to risk rate all client relationships including those in existence prior to 29th December 2000 ("existing customers"). Licensees should review the KYC documentation in relation to their existing customers to ensure compliance with the FTRA, the FTRR and the Licensee's internal KYC requirements. All risk ratings should be documented.

V - VERIFICATION OF CUSTOMER IDENTITY

42 Identity generally means a set of attributes which uniquely define a natural or legal person. There are two main constituents of a person's identity, remembering that a person may be any one of a range of legal persons (an individual, body corporate, partnership, etc). For the purposes of these Guidelines the two elements are :

- the physical identity (eg name, date of birth, registration number); and
- the activity undertaken**.**

Two important aspects of knowing your customer are:

(a) to be satisfied that a prospective customer is who he/she claims to be and is the ultimate client; and,

(b) to ensure that sufficient information is obtained on the nature of the business that the customer expects to undertake, and any expected, or predictable pattern of transactions. This information should be updated as appropriate, and as opportunities arise.

Nature and scope of activity

43 Another important element in verifying a person's identity and establishing adequate due diligence is obtaining and recording sufficient information about the nature of the business that the customer expects to undertake and any expected or predictable, pattern of transactions. For some businesses these may be obvious, however, for more complex businesses this may not be the case. The extent of the description required will depend on the Licensee's own understanding of the applicant's business.

44 When commencing a business relationship, Licensees should record the purpose and reason for establishing the business relationship, and the anticipated level and nature of activity to be undertaken. The extent of documentary evidence will depend on the nature of the product or service. Documentation about the nature of the applicant's business should also cover the origin of funds to be used during the relationship.

For example, funds may be transferred from a bank or the applicant's employer, or be the proceeds of a matured insurance policy.

45 Once a business relationship has been established, reasonable steps should be taken by the Licensee to ensure that descriptive due diligence information is kept up to date as opportunities arise. It is important to emphasise that the customer identification process does not end at the point of application.

When considering entering into a business relationship, certain principles should be followed when ascertaining the level of identification and verification checks to be completed. See Appendix C for a flow chart summary of the different steps involved.

Reasonable measures should be taken to obtain sufficient information to distinguish those cases in which a business relationship is commenced or a *transaction* is conducted with a person acting on behalf of others.

Whenever appropriate and practical the prospective customer should be interviewed personally. If the prospective client fails or is unable to provide adequate evidence of identity or in circumstances in which the Licensee is not satisfied that the transaction for which it is or may be involved is bona fide, an explanation should be sought and a judgment made as to whether it is appropriate to continue the relationship, what other steps can be taken to verify the client's identity and whether or not a report to the FIU ought to be made.

In circumstances in which the relationship is discontinued, funds held to the order of the prospective client should be returned only to the source from which they came and not to a third party.

WHO SHOULD LICENSEES VERIFY

Facility Holder

46 The person whose identity must be verified is described throughout these Guidelines as a "facility holder", "customer" or "client". Who this is will vary. For example:

- a customer dealing on his own behalf is clearly the facility holder;

- when a customer is acting as agent for a principal (for example, as authorised manager of a discretionary investment service for clients) and deals in his own name on behalf of an underlying client, then it is the customer acting as the agent, and not his client, who is the Licensee's facility holder. The underlying client may well be, in turn, a facility holder so far as the agent is concerned;

- when a person wants an investment to be registered in the name of another (e.g. a grandchild), it is the person who provides the funds who should be regarded as the facility holder, rather than the registered owner;

- when an intermediary introduces a client to a Licensee, but the client's name rather than that of the intermediary is given as the investor, it is the client who is the Licensee's facility holder;

- when an individual claiming to represent a company, or another legal entity applies for the use of a facility, then the facility holder will be the entity, the identity or existence of which should be verified, rather than that of any individual claiming to represent it;

- when a company manager or financial and corporate service provider opens a facility on behalf of a client company, it is the client company which is the facility holder;

- in the case of partnerships, the individual partners are joint facility holders; and,

- when a trust or foundation is introduced, it is the settlor or the founder, as the case may be, that is the facility holder.

47 These distinctions are important since they are relevant in determining the correct procedures for verification of identity where this is required.

WHEN MUST IDENTITY BE VERIFIED

48 Where evidence of identity is required, Licensees should verify the identity of their customers as follows:

- in the case of prospective customers, Licensees must verify customer identity before permitting such customers to become facility holders;

- whenever the amount of cash involved in an occasional transaction exceeds $15,000, the identity of the person who conducts the transaction should be verified before the transaction is conducted;

- whenever the amount of cash involved in an occasional transaction exceeds $15,000 and it appears to a Licensee that the person conducting the transaction is doing so on behalf of any other person or persons. In these circumstances the identities of the third parties must be verified before the transaction is conducted; and,

- whenever it appears that two or more (occasional) transactions are or have been deliberately structured to avoid lawful verification procedures in respect of the person(s) conducting the transaction(s) and the aggregate amount of cash involved in the transaction(s) exceed $15,000. Verification should be conducted as soon as practicable after the Licensee becomes aware of the foregoing circumstances.

49 The identity of third parties should be verified before transactions are conducted, or as soon as practicable after Licensees become aware of any of the relevant circumstances referred to above.

50 Where satisfactory evidence of identity is required, a Licensee should "freeze" the rights attaching to the transaction pending receipt of the necessary evidence. The investor may continue to deal as usual, but, in the absence of the evidence of identity, proceeds should be retained. Documents of title should not be issued, nor income remitted (though it may be re-invested).

IDENTIFICATION PROCEDURES

Natural Persons

51 A Licensee should obtain and document the following information when seeking to verify identity:

(i) full and correct name/names used;

(ii) correct permanent address including postcode, (if appropriate);

(iii) date and place of birth;

(iv) nationality;

(v) occupation;

(vi) purpose of the account;

(vii) estimated level of account activity;

(viii) source of wealth (i.e. how the customer acquired his wealth); and,

(ix) source of funds (i.e. generated from what transaction or business and how and by what means the customer intends to transfer the funds/assets to the facility).

Verification of name and address

52 One or more of the following steps is recommended to verify addresses:

- checking the Register of Electors;
- provision of a recent utility bill, tax assessment or bank or credit union statement containing details of the address (to guard against forged copies' it is strongly recommended that original documents are examined);
- checking the telephone directory; and,
- record of home visit.

53 The information obtained should demonstrate that a person of that name exists at the address given, and that the facility holder is that person.

54 Both residence and nationality should be established to ensure that the facility holder is not from a nation that is subject to sanctions by the

United Nations or similar prohibition from any other official body or government that would prohibit such business being transacted. (Licensees should refer to Appendix B for a list of websites which contain information on the status of sanctions.]

55 Obtaining a customer's date of birth provides an extra safeguard if, for example, a forged or stolen passport or driver's licence is used to confirm the identity which bears a date of birth that is clearly inconsistent with the age of the person presenting the document.

56 Confirmation of a person's address and/or nationality is also useful in determining whether a customer is resident in a high-risk country.

57 Information and documentation should be obtained and retained to support, or give evidence to, the details provided by the facility holder.

58 Identification documents, either originals or certified copies, should be pre-signed and bear a discernable photograph of the applicant, for example:

(a) Current valid passport;

(b) Armed Forces ID card;

(c) Drivers licence bearing the photograph and signature of the applicant;

(d) Voter's card;

(e) National Identity card; or

(f) Such other documentary evidence as is reasonably capable of establishing the identity of the individual customer.

59 Where a passport is taken as evidence, the relevant pages should be copied and filed.

When is further verification of identity necessary?

60 Where a customer's identity has been verified, further verification is mandatory if:

(a) during the course of the business relationship the financial institution has reason to doubt the identity of the customer;

(b) a Licensee knows, suspects or has reasonable grounds to suspect that a customer is conducting or proposes to conduct a transaction which:

- involves the proceeds of criminal conduct as defined in the POCA; or

- is an attempt to avoid the enforcement of the POCA.

In such cases, verification should take place as soon as practicable after the Licensee has knowledge or suspicion in respect of the relevant transaction.

(c) there is a material change in the way a facility is operated; and,

61 Licensees may wish, as part of their own internal AML and KYC policies, to re-verify a customer's identity on the occurrence of any of the following "trigger events":

(b) a significant transaction (relative to a relationship);

(c) a material change in the operation of a business relationship;

(d) a transaction which is out of keeping with previous activity;

(e) a new product or account being established within an existing relationship;

(f) a change in an existing relationship which increases a risk profile (as stated earlier);

(g) the early redemption of a fixed term product;

(h) the assignment or transfer of ownership of any product;

(i) the addition of or a change to a principal in any relationship; and

(j) the roll-over of any fixed term product (taking into account the length of the roll-over period).

The above list should not be considered exhaustive.

62 The need to confirm and update information about identity, such as changes of address, and the extent of additional KYC information to be collected over time will differ between firms within any sector. It will also depend on the nature of the product or service being offered, and whether personal contact is maintained enabling file notes of discussions to be made or whether all contact with the customer is remote.

Persons without standard identification documentation

63 Most people need to make use of the financial system at some point in their lives. It is important, therefore, that the elderly, the disabled, students and minors, or the socially or financially disadvantaged should not be precluded from obtaining financial services just because they do not possess the usual types of evidence of identity or address, such as a driver's licence or passport where they cannot reasonably be expected to do so. Internal procedures must allow for this, and must provide appropriate advice to staff on how identity can be confirmed in these exceptional circumstances.

In these circumstances, a common sense approach and some flexibility without compromising sufficiently rigorous AML procedures is recommended. The important point is that a person's identity can be verified from an original or certified copy of another document, preferably one with a photograph.

In these cases it may be possible for the Licensee to accept confirmation from a professional (e.g. doctor, lawyer, etc) who knows the person. Where the individual lives in accommodation for which the person is not financially responsible, or for which there would not be documentary evidence of the person's address, it may be acceptable to obtain a letter from the Department of Social Services or a similar organisation as confirmation of such person's address. A manager may authorise the opening of a business relationship if the manager is satisfied with confirmation of identity circumstances but the decision leading to the authorization must be recorded on the customer's file. Licensees must

also retain this information in the same manner and for the same period of time as other identification records.

64 For students or other young people, the normal identification procedures set out above should be followed as far as possible. Where such procedures would not be relevant, or do not provide satisfactory evidence of identity, verification might be obtained in the form of the home address of parent(s), or by making enquiries of the applicant's college or university. However, care should be taken around the beginning of the academic year before a student has taken up residence at the place of education as registration frauds are known to occur.

65 Under normal circumstances, a family member or guardian who has an existing relationship with the Licensee concerned would introduce a minor. In cases where the person opening the account is not already known, the identity of that person, and any other person who will have control of the account, should be verified.

66 Licensees should also take appropriate steps to verify the name and address of applicants by one or more methods, e.g.:

(i) obtaining a reference from a "respected professional" who knows the applicant;

(ii) checking the voter's card;

(iii) making a credit reference agency search;

(iv) checking a local telephone directory;

(v) requesting sight of a recent real property tax bill, local authority tax bill, utility bill, bank, credit union or trust company statement.(To guard against forged or counterfeit documents, care must be taken that the document is an original and not a copy); or

(vi) personal visit to the home of the applicant where possible.

67 The term 'respected professional' could refer to for instance, lawyers, accountants, directors or managers of a regulated Licensee, priests, ministers, doctors or teachers.

68 Where a proposed facility holder's address is temporary accommodation, for example an expatriate on a short term overseas contract, Licensees should adopt flexible procedures to obtain verification under other categories, such as copy of contract of employment, or banker's or employer's written confirmation.

Certification of identification documents

69 Where possible, face-to-face customers must show Licensees' staff original documents bearing a photograph, and copies taken immediately and retained and certified by a senior staff member**.**

70 Where it is impractical or impossible to obtain sight of original documents, a copy is acceptable where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the facility holder.

71 A certifier must be a suitable person, such as for instance:

- Certified Public Accountant;
- Bank or Trust Company Official;
- Counsel and Attorney-at-Law;
- Senior Civil Servant;
- Doctor of Medicine;
- Justice of the Peace;
- Member of the House of Assembly;
- Minister of Religion;
- Notaries Public;
- Police Officer; or
- Teacher

The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address, telephone and facsimile number and where applicable, a license/registration number.

72 The list above of suitable certifiers is not intended to be exhaustive, and Licensees should exercise due caution when considering certified copy documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. Where certified copy documents are accepted, it is the Licensee's responsibility to satisfy itself that the certifier is appropriate. In all cases, Licensees should also ensure that the customer's signature

on the identification document matches the signature on the application form, mandate, or other document.

73 Because documents providing photographic evidence of identity need to be compared with the applicant's appearance, and to guard against the dangers of postal intercept and fraud, prospective customers should not be asked to send their identity documents by post.

74 Where there is no face-to-face contact, and photographic identification would clearly be inappropriate, procedures to identify and authenticate the customer should ensure that there is sufficient evidence, either documentary or electronic, to confirm address and personal identity. At least one additional check should be undertaken to guard against impersonation. In the event that internal procedures require sight of a current passport or ID Card where there is no face-to-face contact, then copies certified by a suitable certifier should be obtained:

75 There are obviously a wide range of documents which might be provided as evidence of identity. It is for each Licensee to decide the appropriateness of any document in the light of other procedures adopted. However, particular care should be taken in accepting documents which are easily forged or which can be easily obtained using false identities.

76 Any subsequent change to the customer's name, address, or employment details of which the Licensee becomes aware should be recorded and also be regarded as a "trigger" event. Generally a KYC review would be undertaken as part of good business practice and due diligence process but it would also serve for money laundering prevention.

77 File copies of supporting evidence should be retained. Licensees that regularly conduct one-off transactions, should record the details in a manner which allows cross reference to transaction records. Such Licensees may find it convenient to record identification details on a separate form, to be retained with copies of any supporting material obtained.

78 An introduction from a respected customer personally known to the management, or from a trusted member of staff, may assist the verification procedure but does not replace the need for verification of address as set out above. Details of the introduction should be recorded on the customer's file.

Corporate Clients

79 It will normally be necessary to obtain the following documented information concerning corporate clients:

(i) Certificate of Incorporation or equivalent document;

(ii) Memorandum and Articles of Association;

(iii) Description and nature of the corporate entity's business including:

(a) date of commencement of business;

(b) products or services provided;

(c) location of principal business; and,

(d) name and location of the registered office and registered agent of the corporate entity.

(iv) The reason for establishing the business relationship;

(v) The potential parameters of the account including:

(a) size in the case of investment and custody accounts;

(b) balance ranges, in the case of current and deposit accounts;

(c) an indication of the expected transaction volume of the account;

(d) the source of wealth;

(e) the source of funds;

(f) a copy of the last available financial statements audited where applicable.

(vi) Satisfactory evidence of the identity of each of those beneficial owners having a controlling interest in the corporate entity

(other than a publicly traded company), being any person holding 10% interest or more or with principal control over the company's assets and any person (or persons) on whose instructions the signatories on the account are to act or may act where such persons are not full time employees, officers or directors of the company;

(vii) In the case of a bank account, satisfactory evidence of the identity of the account signatories, details of their relationship with the company and if they are not employees an explanation of the relationship. All signatories must be verified;

(viii) Evidence of the authority to enter into the business relationship, for example, a copy of the Board Resolution authorising the opening of the account or other facility and the signatories authorized to sign on the account;

(ix) Copies of Powers of Attorney, or any other authority, affecting the operation of the account given by the directors in relation to the company and supported by a copy of the respective Board Resolution;

(x) Copies of the list/register of directors and officers of the corporate entity including their names and addresses; and,

(xi) Satisfactory evidence of identity must be established for at least two (2) directors, one of whom should if applicable, be an executive director where different from account signatories.

80 It is sometimes a feature of corporate entities being used to launder money that account signatories are not directors, managers or employees of the corporate entity. In such circumstances, Licensees should exercise caution, making sure to verify the identity of the signatories, and where appropriate, monitoring the ongoing business relationship more closely.

81 Where it is impractical or impossible to obtain sight of the original Certificate of Incorporation or equivalent, Licensees may accept a suitably certified copy in accordance with the procedures stated in paragraphs 69 to 73 of these Guidelines.

82 Trading companies may sometimes form part of complex organisational structures which also involve trusts and foundations. Particular care

should be taken to verify the legal existence of the corporate entity and to ensure that any person purporting to act on behalf of the corporate entity is authorised to do so. The principal requirement is to look behind a corporate entity to identify those who have ultimate control over the business and the company's assets, with particular attention being paid to any shareholders or others who exercise a significant influence over the affairs of the company. Enquiries should be made to confirm that the company exists for a legitimate trading or economic purpose, and that it is not merely a "brass plate company" where the controlling principals cannot be identified.

83 Before a business relationship is established, measures should be taken by way of company search and/or other commercial enquiries to ensure that the applicant company has not been, or is not in the process of being, dissolved, struck off, wound-up or terminated. In addition, if the Licensee becomes aware of changes in the company structure or ownership, or suspicions are aroused by a change in the nature of business transacted, further checks should be made.

84 Where the business relationship is being opened in a different name from that of the corporate entity, the Licensee should also make a search, of equivalent trading name search for the second name.

85 The following persons (i.e. individuals or legal entities) must also be identified in line with this part of the Guidelines:

(i) All of the directors who will be responsible for the operation of the account/transaction;

(ii) All the authorized signatories for the account/transaction;

(iii) All holders of powers of attorney to operate the account/transaction;

(iv) The beneficial owner(s) of the company; and,

(v) The majority shareholder(s) of the company (if different from the beneficial owner[s].

86 Where persons are already known to the Licensee and identification records are already in compliance with the requirements of these Guidelines, there is no need to verify identity again.

87 When authorised signatories change, care should be taken to ensure that the identities of all current signatories have been verified. In addition, it may be appropriate to make periodic enquiries to establish whether there have been any changes in directors/shareholders, or the nature of the business/activity being undertaken. Such changes could be significant in relation to potential money laundering activity, even though authorised signatories have not changed.

88 Bearer shares present an additional risk to financial institutions. Without adequate safeguards in place it is impossible for the Licensee to know with certainty that the true identity of the beneficial owner(s) has been disclosed to them.

89 The use of bearer shares should be discouraged. However, where the proposed customer is a company with bearer shares in issue, the Licensee should ensure that physical control of the shares is held by the Licensee itself or by an appropriate third party (who should provide the Licensee with an undertaking to complete and forward new verification documentation immediately upon transfer of any interest in the shares).

90 Where the corporate client is a segregated accounts company, Licensees should have regard to the guidance contained in the preceding paragraphs (paragraphs 79 to 89). In addition to the documented information set out in paragraph 79, Licensees should also obtain a copy of the Registrar General's certificate of registration to confirm the existence and legal standing of the segregated account company.

Powers of attorney

91 The authority to deal with assets under a power of attorney constitutes a business relationship and therefore, where appropriate, Licensees should verify the identities of holders of powers of attorney, the grantor of the power of attorney and third party mandates. Records of all transactions undertaken in accordance with a power of attorney should be kept in accordance with Section VI of these Guidelines.

Partnerships/Unincorporated Businesses

92 It will normally be necessary to obtain the following documented information concerning partnerships/Unincorporated Businesses:

(i) Identification evidence for all partners/controllers of a firm or business, who are relevant to their firm's application to become a facility holder and who have individual authority to operate a facility or otherwise to give relevant instructions;

(ii) Identification evidence for all authorised signatories, in line with the requirements for individual customers. When authorised signatories change, care should be taken to ensure that the identity of the current signatories has been verified.

(iii) Description and nature of the business including:

a) name of business;

b) date of commencement of business;

c) products or services provided; and,

d) location of principal place of business;

(iv) The reason for establishing the business relationship and the potential parameters of the account including:

a) size in the case of investment and custody accounts;

b) balance ranges, in the case of current and deposit accounts;

c) an indication of expected transaction volume of the account;

e) source of funds;

f) source of wealth; and,

g) a copy of the last available financial statements (audited where applicable).

(v) An explanation of the nature of the business or partnership should be ascertained (and if possible verified from a partnership deed) to ensure that it has a legitimate purpose. Where a formal partnership arrangement exists, a mandate from the partnership authorising the opening of an account or the use of some other

facility and conferring authority on those who will undertake transactions should be obtained.

Financial and Corporate Service Providers

93 Licensees are required to verify the identity of financial and corporate service providers ("FCSPs") licensed under the Financial and Corporate Service Providers Act, 2000 ("the FCSPA"). Licensees should also, in accordance with the FTRA, verify the identity of any clients of an FCSP where the FCSP operates a facility, such as for example, an omnibus account, on behalf of its client.

94 In the case of FCSPs, Licensees should adhere to the following guidance when conducting due diligence on a FCSP:

(i) where a FCSP is a natural person, Licensees should follow the guidance set out in paragraphs 51 to 59;
(ii) where a FCSP is a corporate client, Licensees should follow the guidance set out in paragraphs 79 to 89, and
(iii) where a FCSP is a partnership or unincorporated association, Licensees should follow the guidance set out in paragraph 92.

In each case, a copy of the FCSP's licence should be obtained in order to confirm the existence and legal standing of the FCSP.

95 Where a FCSP holds funds on behalf of their clients in a client or omnibus account, Licensees should adhere to the guidance set out in paragraphs 131 and 132.

Legal Structures and Fiduciary Arrangements

96 Legal structures such as trusts and Foundations, and nominee and fiduciary accounts can be used by criminals who wish to mask the origin of funds derived from crime if the trustee or fiduciary does not carry out adequate procedures. Particular care is needed on the part of the Licensee when the facility holder is a trustee or fiduciary who is not an Exempted Client (see paragraph 155) or an Eligible Introducer (see paragraph 147). The principal means of preventing money laundering through the use of legal structures, nominee companies, and fiduciaries is to verify the identity of the provider of funds, such as the settlor and

also those who have control over the funds, that is to say, the trustees, advisors, and any controllers who have the power to remove the trustees/advisors etc.

In such cases the Licensee should normally, in addition to obtaining identification evidence for the trustee(s) and any other person who has signatory powers on the account:

(i) make appropriate enquiry as to the general nature and the purpose of the legal structure and the source of funds;

(ii) obtain identification evidence for the settlor(s); and,

(iii) in the case of a nominee relationship, obtain identification evidence for the beneficial owner(s).

97 In some cases it may be impractical to obtain all of the above (e.g. if the settler has died). Discretion must be exercised but in a manner consistent with the spirit of these Guidelines. Licensees providing trustee and fiduciary services should refer to paragraph 96 of these Guidelines.

98 For discretionary trusts, the nature and purpose of the trust and the original source of funding should be ascertained.

99 Particular care needs to be exercised when legal structures such as trusts, foundations, special purpose vehicles, or international business companies connected to trusts or foundations, are established. Those created in jurisdictions without equivalent money laundering procedures in place will warrant additional enquiry.

100 Licensees should obtain written confirmation from the trustees/managers/advisors of the legal structures that there are no anonymous principals.

101 Any application to open an account, or undertake a transaction, on behalf of another without the applicant identifying a trust or nominee capacity should be regarded as suspicious and should cause the need of further enquiries.

102 Licensees are also required by the FTRA to verify the identity of any underlying beneficiary of a legal structure where the beneficiary has a

vested interest in the legal structure, (for avoidance of any doubt, the foregoing verification need not be implemented where such beneficiary is only entitled to receive an interest under e.g. a trust and is not, or does not wish to become, a facility holder). Such verification must be carried out by the Licensee providing the facility unless the transaction is or has been introduced by another financial institution (as described in paragraph 147 of these guidelines) on behalf of the settlor and beneficiary and such financial institution is itself required to verify the identity of the settlor and beneficiary.

103 Licensees should be particularly vigilant where there is no readily apparent connection or relationship of the settler to the beneficiaries of a trust. Since the economic nature of a trust is a mechanism for the settler to benefit a beneficiary, typically, not in return for any consideration (payment, transfer of assets or provision of services), Licensees should endeavour so far as possible to ascertain the settlor's reasons for wanting to benefit a beneficiary with whom he seemingly has no connection. This can be a matter of great sensitivity (fpr example where the beneficiary turns out to be a child of the settlor born out of wedlock) and Licensees are encouraged to take this into account while pursuing necessary or appropriate inquiries.

Conventional Family and Absolute Trusts

104 In the case of conventional trusts, identification documents should be obtained for:

(i) those who have control over the funds i.e. the principal trustees (which may include the settlor); and,

(ii) the provider of the funds i.e. the settlor (except where the settlor is deceased).

105 Where the settlor is deceased, written confirmation should be obtained for the source of funds in the form, for example, of grant of probate, and/or copy of the will creating the trust.

106 Where a corporate trustee acts jointly with a co-trustee, the identity of any non-regulated co-trustees should be verified even if the corporate trustee is covered by an exemption. The relevant guidance contained in

this section for verifying the identity of persons, unincorporated associations or companies should be followed.

107 Copies of any documents should be certified as true copies. In addition, a cross check should be made to ensure that any bank account on which the trustees have drawn funds is in their names, and the identities of any additional authorised signatories to the bank account should also be verified.

Identification of New Trustees

108 Where a trustee whose identity has been verified is replaced, the identity of the new trustee should be verified before the new trustee is allowed to exercise control over funds.

Foundations

109 It will normally be necessary to obtain the following documented information concerning foundations:

(i) The foundation's charter

(ii) The Registrar General's certificate of registration should be obtained in order to confirm the existence and legal standing of the foundation

(iii) The source of wealth;

There may be cases when a person other than the founder provides funds for the foundation. Licensees should therefore obtain and document information on the source of funding for the foundation and should verify the identity of any third party providing the funds for the foundation and/or for whom a founder may be acting;

(iv) Licensees should obtain identification evidence for the founder(s) and for such officers and council members as may be signatories for the account(s) of the foundation. Where the founder is a company, Licensees should have regard to the guidance on corporate clients contained in paragraphs 79 to 89; where the founder is an individual, licensees should follow the guidance provided in paragraphs 51 to 59.

110 Identification evidence should also be obtained for the beneficiaries of the foundation, where these are designated in the foundation charter or named as such by the foundation council or by the person or body appointed for this purpose in the charter.

Executorship Accounts

111 Where a business relationship is entered into for the purpose of winding up the estate of a deceased person, the identity of the executor(s)/administrator(s) of the estate should be verified in line with this guidance, depending on the nature of the executor (i.e. whether personal, corporate, or a firm of attorneys). However, the identity of the executor or administrator need not normally be verified when payment from an established bank account in the deceased's name is being made to the executor or administrator in accordance with the Grant of Probate or Letters of Administration solely for the purpose of winding up the estate. Payments to the underlying beneficiaries on the instructions of the executor or administrator may be made without verification of their identity.

112 If any suspicions are aroused about the nature or origin of assets comprising an estate that is being wound up, then a report of the suspicions should be made to the FIU in accordance with the procedures set out in the FIU's Suspicious Transactions Reporting Guidelines.

Non-profit Associations (including charities)

113 Non-profit associations may pose specific risks of money laundering for Licensees. At the placement stage there may be difficulties in identifying the source of funds, the identity of the donor, and verifying the information where it is provided. In some circumstances, such as in the case of anonymous donations, the identity of the donor is not known and as a result neither is the source of the funds.

114 Where the entity is a corporate entity the account opening procedures should be in accordance with the procedures for corporate clients set out in paragraphs 79 to 89, in the case of Trusts the procedures in paragraphs 96 to 103 and, in the case of Foundations the procedures in paragraphs 109 and 110 should be followed.

115 Where a facility holder is a non-profit association, it will normally be necessary to obtain the following documented information:

(i) An explanation of the nature of the proposed entity's purposes and operations; and,

(ii) the identity of at least two signatories and/or anyone authorized to give instructions on behalf of the entity should be obtained and verified.

116 Where a non-profit association is registered as such in an overseas jurisdiction, it may be useful for the Licensee to contact the appropriate charity commission or equivalent body, to confirm the registered number of the charity and to obtain the name and address of the commission's correspondent for the charity concerned. Licensees should satisfy themselves as to the legitimacy of the organization by, for example, requesting sight of the constitution.

117 Licensees should refer to Appendix B for a list of relevant websites which provide information on non-profit organizations and charities.

118 Whilst it is not practical to obtain documentary evidence of identity of all donors, Licensees should undertake a basic "vetting" of all non-profit associations established in other jurisdictions, in relation to known money laundering and terrorist activities. This includes a reasonable search of public information; verifying that the non-profit association does not appear on any terrorist lists nor that it has any association with money laundering and that identification information on representatives /signatories is obtained. Licensees are advised to consult the websites listed in Appendix B. Particular care should be taken where the purposes to which the associations' funds are applied are located in a high-risk country (see paragraphs 127 and 128 below).

Investment Funds

119 It will normally be necessary to obtain the following documentation concerning the Investment Fund:

(i) Certified copy of the Investment Fund License;

(ii) Written confirmation from the Investment Fund Administrator that the identity of the Directors and Promoters has been carried out in accordance with the provisions of the FTRA and FTRR;

(iii) Undertaking from the Investment Fund Administrator that they will advise the Licensee of any material changes to the Investment Fund;

(iv) Undertaking from the Investment Fund Administrator that should the Licensee require the documents necessary to verify the identity of the Promoters or Directors, the Investment Fund Administrator shall provide the Licensee with such information;

[v] Certificate of Incumbancy, detailing names and addresses of Directors;

(vi) Certificate of Good Standing;

(vii) Offering Document;

(viii) Certified copy of Certificate of Incorporation;

(ix) Certified copy of Memorandum and Articles of Association;

(x) Resolution appointing first Directors and any subsequent Directors;

(xi) Resolution of Directors authorizing opening of account.

Politically Exposed Persons ("PEPs")

120 Business relationships with individuals holding important public positions and with related parties (eg. close family members or related companies) may expose Licensees to significant reputational and/or legal risk. The risk occurs when such persons abuse their public powers for either their own personal benefit and/or the benefit of others through illegal activities such as the receipt of bribes or fraud. Such persons commonly referred to as 'politically exposed persons' or 'potentates' include heads of state, government ministers, influential public officials, judges and military commanders.

121 Provision of financial services to corrupt PEPs exposes Licensees to reputational risk and costly law enforcement measures.

122 Licensees are encouraged to be vigilant in relation to PEPs from all jurisdictions, in particular High Risk Countries (see paragraphs 127 and 128), who are seeking to establish business relationships. In relation to PEPs, in addition to performing normal due diligence measures, Licensees should:

(i) have appropriate risk management systems to determine whether the customer is a PEP;

(ii) have developed a clear policy and internal guidelines, procedures and controls regarding such business relationships;

(iii) obtain senior management approval for establishing business relationships with such customers;

(iv) take reasonable measures to establish the source of wealth and source of funds; and,

(v) ensure the proactive monitoring of the activity on such accounts, so that any changes are detected, and consideration can be given as to whether such changes suggests corruption or misuse of public assets.

123 Licensees should ensure that timely reports are made to the FIU where proposed or existing business relationships with PEPs give grounds for suspicion.

124 Licensees should develop and maintain "enhanced scrutiny" practices to address PEPs risk:

(i) Licensees should assess country risks where they have financial relationships, evaluating, *inter alia,* the potential risk for corruption in political and governmental organizations. (See the information set out in Appendix B). Licensees which are part of an international group might also use the group network as another source of information.

(ii) Where Licensees entertain business relations with entities and nationals of countries vulnerable to corruption, they should establish who the senior political figures are in that Country, and should also seek to determine, whether or not their customer has any connections with such individuals (for example immediate family or close associates). Licensees should note the risk that customer relationships may be susceptible to acquiring such connections after the business relationship has been established.

(iii) Financial services businesses should be most vigilant where their customers are involved in those businesses which appear to be most vulnerable to corruption, such as, but not limited to trading or dealing in precious stones or precious metals.

125 In particular detailed due diligence, should include:

(a) Close scrutiny of any complex structures (for example, involving legal structures such as corporate entities, trusts, foundations and multiple jurisdictions);

(b) Every effort to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship, both at the outset of the relationship and on an ongoing basis;

(c) The development of a profile of expected activity on the business relationship so as to provide a basis for future monitoring. The profile should be regularly reviewed and updated;

(d) A review at senior management or board level of the decision to commence the business relationship and regular review, on at least an annual basis, of the development of the relationship; and,

(e) Close scrutiny of any unusual features, such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, the use of unknown financial institutions and regular transactions involving sums just below a typical reporting level.

126 There should be full documentation of the information collected in line with Licensees' policies to avoid or close business relationships with

PEPs. If the risks are understood and properly addressed then the acceptance of such persons becomes a business/commercial decision as with all other types of customers. Licensees should refer to Appendix B for a list of websites relevant to the risks associated with PEPs.

High-Risk Countries

127 Certain countries are associated with predicate crimes such as drug trafficking, fraud and corruption and consequently pose a higher potential risk to Licensees. Conducting business relationships with customers who are either citizens of or domiciled in such countries exposes the Licensee to reputational risk and legal risk.

128 Caution should also be exercised in respect of the acceptance of certified documentation from individuals and entities located in high-risk countries and territories and appropriate verification checks undertaken on such individuals/entities to ensure their legitimacy and reliability.

Products & Services Requiring Special Consideration

129 Special consideration should be given to the provision of the following products and services:

(a) Provision of safe custody and safety deposit boxes

130 Where facilities to hold boxes, parcels and sealed envelopes in safe custody are made available, it is expected that Licensees will follow the identification procedures set out in these Guidelines.

(b) Intermediaries

131 The FTRA requires Licensees to not only verify the identity of an intermediary but also to look through that entity to the underlying client(s). Where the intermediary is not one of the financial institutions referred to in paragraph 147 of these Guidelines and/or is from a country that is not listed in the First Schedule of the FTRA, measures must be taken to verify the identity of the underlying clients. In satisfying this requirement, the Licensee should have regard to the nature of the intermediary, the domestic regulatory regime in which the intermediary operates and the financial institutions' confidence in it, to its

geographical base and to the type of business being done. Where however, the intermediary is one of the financial institutions referred to in paragraph 147, such verification is not required.

132 Broker dealers, investment fund administrators, counsel and attorneys, accountants, estate agents and other intermediaries frequently hold funds on behalf of their clients in "client accounts" opened with Licensees. Such accounts may be pooled omnibus accounts holding the funds of many clients, or they may be opened specifically for a single client or for a number of clients, either undisclosed to the Licensee or identified for reference purposes only. In each case, it is the intermediary who is the Licensee's customer and these situations should be distinguished from those where an intermediary introduces a client and where that client becomes the customer of the Licensee.

(c) Correspondent Relationships

133 Transactions conducted through correspondent relationships need to be monitored according to perceived risk. "Know Your Correspondent" procedures should be established to ascertain whether the correspondent bank or counter-party is itself regulated for money laundering prevention and, if so, whether the correspondent is required to verify the identity of customers in accordance with standards which are at least equivalent to the standards required under Bahamian law. Where this is not the case, additional due diligence would be required to ascertain and assess the correspondent's internal policy on AML and KYC procedures. Licensees must not maintain relationships with banks that have no physical presence in any country or with correspondent banks that permit their accounts to be used by such banks.

134 The volume and nature of transactions flowing through correspondent accounts with Licensees from high risk jurisdictions, or those with material deficiencies should be monitored against expected levels and destinations, and any material variances should be explored.

135 Staff dealing with correspondent banking accounts should be trained to recognise high risk circumstances, and be prepared to challenge correspondents over irregular activity, whether isolated transactions or trends, submitting an STR where appropriate.

136 Licensees should consider terminating the accounts of correspondents who fail to provide satisfactory answers to reasonable enquiries

including, where appropriate, confirming the identity of customers involved in unusual or suspicious transactions.

137 A review of the correspondent bank relationship should be conducted at least annually.

(d) Occasional Transactions

138 It is important for Licensees to determine whether a facility holder is undertaking an occasional transaction, or whether the transaction is the initial step in an ongoing business relationship as this can affect the verification requirements. The same transaction may be viewed differently by a Licensee, and by an introducing intermediary, depending on their respective relationships with the facility holder. Therefore, where a transaction involves an intermediary, both the Licensee and the intermediary must separately consider their positions, and ensure that their respective obligations regarding verification of identity and associated record keeping are met.

139 The FTRA defines an "occasional transaction" as, *inter alia,* any transaction which is not conducted through a facility held by a customer.

140 Customers who conduct occasional transactions (whether a single transaction or a series of linked transactions) where the amount of the transaction or the aggregate of a series of linked transactions is less than $15,000 or the equivalent in any other currency, are exempt from the verification requirements of the FTRA.

141 Licensees need to be aware at all times of any cases where the total of a series of linked transactions exceeds the prescribed limit of $15,000 and they should verify the identity of the customer in such cases. These are cases where in respect of two or more occasional transactions it appears at the outset, or at a later stage, to a person handling any of the transactions that the transactions are linked and that the aggregate amounts of these transactions exceed or are likely to exceed $15,000.

142 As a matter of best practice, a time period of 3 months for the identification of linked transactions is normally acceptable. However there is some difficulty in defining an absolute time scale that linked transactions may fall within. Therefore the relevant procedures for linking will ultimately depend on the characteristics of the product rather

than relating to any arbitrary time limit. For example, Licensees should be aware of any obvious connections between the sender of funds and the recipient.

143 Verification of identity will not normally be needed in the case of an exempted occasional transaction referred to above. If, however, the circumstances surrounding the occasional transaction appear to the Licensee to be unusual or questionable, further enquiries should be made. If as a result of enquiries, the licensee becomes aware of or suspects money laundering the Licensee must, in accordance with section 10(A)(1) of the FTRA, take steps to verify the proposed client's identity. Where money laundering is known or suspected, the Licensee should make a suspicious transaction report in line with Section 14(1) of the FTRA regardless of the size of the transaction.

RELIANCE ON THIRD PARTIES TO CONDUCT KYC FOR CUSTOMERS

144 Every Licensee must retain adequate documentation to demonstrate that its KYC procedures have been properly implemented, and that it has carried out the necessary verification itself. There are, however, certain circumstances in which it may be possible for Licensees to rely on KYC procedures carried out by third parties. Whereas the procedures listed below refer to the obtaining and verification of original documentation, they do not exempt Licensees from the requirement to have copies of all documentation in their possession, or to have ready access to such documentation.

145 Licensees may rely on the written confirmation of other financial institutions ("eligible introducers") that they (the other financial institution) have verified customer identity in the instances permitted by the FTRA. Examples of when written confirmation may be relied upon by Licensees are:

(i) Where a Licensee is unable to readily determine whether or not an occasional transaction involves cash because a customer deposited funds into a facility held for and on behalf of the Licensee by an eligible introducer;

(ii) Where an eligible introducer, conducts a transaction on behalf of a customer, using the facilities of a Licensee, the Licensee may rely upon the written confirmation of the eligible introducer that it has

verified the identity of the customer concerned (See section 8(6) and 9(6) FTRA); and,

Where such transactions are conducted through the facilities of an eligible introducer, in addition to obtaining written confirmation, a Licensee must also confirm the existence of the facility provided by the eligible introducer. (See section 11(3) and 11(4) FTRA).

146 This exemption applies only to occasional transactions and transactions conducted by Licensees which are facility holders. However, if the person being introduced is forming a business relationship with the Licensee, then that Licensee must carry out the appropriate due diligence and obtain the necessary evidence of identity.

Introductions from Group Companies or Intermediaries

147 Where a business relationship is being instituted the Licensee is obliged to carry out KYC procedures on any client introduced to it by a third party unless the third party is an eligible introducer able to provide the Licensee with copies of all documentation required by the Licensee's KYC procedures.

To be an eligible introducer, a domestic third party must be one of the following regulated financial institutions

(1) a bank or trust company licensed by the Central Bank of The Bahamas;
(2) a company carrying on life assurance business pursuant to section 2 of the Insurance Act;
(3) a broker-dealer as defined by section 2 of the Securities Industry Act;
(4) an investment fund administrator or an operator of investment fund (as defined by the Investment Funds Act, 2003).

A foreign financial institution may also act as an eligible introducer if it meets all four of the following conditions:

- It must exercise functions similar to those of the financial institutions listed in sub-paragraphs 147 (1) to (4) above;
- It must be subject to equivalent, or more stringent, anti-money laundering legislation than that in place in The Bahamas.
- It must be based in a country listed in the First Schedule to the

FTRA as having equivalent anti-money laundering legislation.

- There must be no secrecy or other obstacles which would prevent the Licensee from obtaining the original documentation if necessary.

148 Where a third party satisfies the definition of eligible introducer, a Licensee may place reliance upon the KYC procedures of the eligible introducer who must be able to supply copies of the relevant documentation as required by the Licensee.

149 Where reliance is to be placed on an eligible introducer, the Licensee remains ultimately responsible for ensuring that adequate due diligence procedures are followed and that the documentary evidence of the eligible introducer is satisfactory for these purposes. Satisfactory evidence is such evidence as will satisfy the anti-money laundering regime in the First Schedule country from which the introduction is made. Copies of all documentation necessary to enable the Licensee to verify the identity of the introduced client must be supplied together with the appropriate Introducer's Certificate.

EXEMPTIONS AND CONCESSIONS

150 Irrespective of the size and nature of the transactions and the exemptions set out below, identity must be verified in all cases where money laundering is known or suspected. If money laundering is known or suspected then a report must be made to the FIU and verification procedures undertaken if this has not already been done.

151 The obligation to maintain procedures for obtaining evidence of identity is general, but paragraphs 152 to 155 set out a number of exemptions and concessions.

Bahamas or foreign Financial Institutions

152 Verification of identity is not normally required when the facility holder is one of the domestic financial institutions referred to in paragraph 147 or, is an equivalent financial institution in a country listed in the First Schedule to the FTRA. Licensees should satisfy themselves that the financial institution does actually exist (e.g. that it is listed in the Bankers' Almanac, or is a member of a regulated or designated investment exchange); and that it is also regulated. In cases of doubt, the relevant regulator's list of Licensees can be consulted. Additional comfort

can also be obtained by obtaining from the relevant Licensee evidence of its authorisation to conduct financial and/or banking business.

In all cases, the Licensee must be satisfied that it can rely upon the eligible introducer. The Licensee may request from an eligible introducer such evidence as it reasonably requires to satisfy itself as to the identity of the introducer and the robustness of its KYC policies and procedures.

153 Other Bahamas or foreign financial businesses (e.g. bureaux de change) should be subject to further verification in accordance with the procedures for companies or businesses.

Occasional Transactions: Single or Linked

154 Verification of identity is not normally needed in the case of a single occasional transaction when payment by, or to, the applicant is less than $15,000. Irrespective of the size of a transaction however, any suspicions of money laundering must be reported in accordance with the FIU's Suspicious Transactions Reporting Guidelines. Licensees should also have regard to paragraphs 138 to 143 of these guidelines when dealing with occasional transactions.

Exempted Clients

155 Documentary evidence of identity will not normally be required in the case of:

(i) Superannuation Schemes;

(ii) Discretionary Trusts;

(iii) Occupational Retirement/Pension Plans which allow non-employee participation;

(iv) Financial institutions regulated by the Central Bank, the Securities Commission of The Bahamas, the Registrar of Insurance, or the Gaming Board;

(v) Foreign financial institutions located in a jurisdiction specified in the First Schedule of the FTRA, which is regulated by a body having equivalent regulatory and supervisory responsibilities as

the Central Bank the Securities Commission of The Bahamas, the Registrar of Insurance, or the Gaming Board;

(vi) any central or local government agency or statutory body;

(vii) a publicly traded company or investment fund listed on The Bahamas International Stock Exchange or any other Stock Exchange specified in the Schedule to the FTRR and approved by the Securities Commission of The Bahamas;

(viii) an applicant for insurance consisting of a policy of insurance in connection with a pension scheme taken out by virtue of a person's contract of employment or occupation;

(ix) an applicant for insurance in respect of which a premium is payable in one installment of an amount not exceeding $2,500;

(x) an applicant for insurance in respect of which a periodic premium is payable and where the total payable in respect of any calendar year does not exceed $2,500;

(xi) any Bahamian dollar facility of or below $15,000.

TREATMENT OF BUSINESS RELATIONSHIPS EXISTING PRIOR TO 29th DECEMBER 2000

156 Section 6(6) of the FTRA, provides that financial institutions are required to verify the identity of customers who have facilities which were established prior to 29th December 2000 ("existing facilities"). Where a Licensee of the Central Bank of The Bahamas had not verified the identity of any such customer by 1st April 2004 ("existing customers"), the Licensee was required to notify the Central Bank not later than 30th April 2004. Licensees should have regard to the paragraphs which follow when dealing with existing facilities:

157 It is clear that certain business relationships established prior to the enactment of the FTRA (29th December, 2000) can still present a major threat of money laundering, and indeed, it is a widely recognised tactic for money launderers to establish seemingly legitimate and normally-run accounts which are then used for laundering money at a later date.

158 Licensees are encouraged to develop and implement the following policies and procedures where information on existing customers is not obtained:

(i) Maintain a record of their non-compliant business relationships and note in each case what information or documentation is missing and the reason or supposed reason for its absence.

(ii) Establish procedures to deal with the business relationship in those situations where satisfactory evidence was not obtained by 1st April 2004 and continue to make reasonable efforts to secure compliance. Licensees should risk rate these relationships in accordance with the requirements of the Section VI of these Guidelines.

(iii) In accordance with section 6(6) of the Financial Transactions Reporting Act, 2000, the Central Bank hereby directs licensees to complete the verification of existing client identity, in the case of domestic retail business, by June 30th 2006 and in the case of all other business by December 31st 2005. Licensees must implement appropriate measures to satisfy the verification requirements of section 6(6) of the FTRA by these dates, or take steps to suspend or terminate the business relationship. Such measures would include, for example, refusing to accept further funds from customers whose identities have not been verified, or providing further services to such persons or suspending the account or other facility held in the customer's name or the termination of the business relationship altogether. Any such action should be carried out if and to the extent that it can properly be done by the Licensee, without prejudicing third parties (including customers who have verified their identity) and without exposing the Licensee to liability, loss or prejudice.

159 The Central Bank will monitor and assess the programs implemented by Licensees to meet the verification requirements of the FTRA by the target dates outlined in paragraph 158(iii) above.

160 Licensees are reminded of the reporting duties imposed by the Financial Transactions Reporting Act, 2000 with respect to suspicious transactions. Where a customer refuses to provide information for his identity to be verified in accordance with the verification requirements of section 6, this may be a circumstance that should put the Licensee on

enquiry as to whether the reason for non-cooperation may be that the business relationship is being used for money laundering purposes.

In those cases where persons do not have standard identification documents some flexibility is suggested in paragraph 63 above. For existing customers, an introduction from a respected customer personally known to a Director, Manager or senior member of staff, will often provide comfort provided that the conditions of paragraph 63 are satisfied and that the introduction can never replace the address verification procedures described in these Guidelines. Details of who initiated the account and authorized the introduction must be kept. Directors/Senior Managers should take a common sense approach in determining whether certain documents should be waived in any particular situation. Where specific documentation of a customer is waived, management must document why the waiver was granted.

161 When an existing customer closes one account and opens another, or enters into a new agreement to purchase products or services, there is no need to verify identity or address. However, the opportunity should be taken to confirm the relevant customer information. This is particularly important if there has been no recent contact or correspondence with the customer e.g. within the last twelve months or when a previously dormant account has been reactivated.

ON-GOING MONITORING OF BUSINESS RELATIONSHIPS

162 Once the identification procedures have been completed and the client relationship is established, Licensees should monitor the conduct of the relationship/account to ensure that it is consistent with the nature of business stated when the relationship/account was opened.

Monitoring

163 Licensees are expected to have systems and controls in place to monitor on an ongoing basis relevant account activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for Licensees to be vigilant to note any significant changes or inconsistencies in the pattern of transactions. Inconsistency is measured against the stated original purpose of the accounts. Possible areas to monitor could be: -

a. transaction type
b. frequency
c. amount
d. geographical origin/destination
e. account signatories

164 It is recognised that the most effective method of monitoring of accounts/business relationship is achieved through a combination of computerised and human manual solutions. A corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring method as a matter of course. Computerised approaches may include the setting of “floor levels" for monitoring by amount.

165 Whilst some Licensees may wish to invest in computer systems specifically designed to assist the detection of fraud and money laundering, it is recognized that this may not be a practical option for many Licensees for the reasons of cost, the nature of their business, or difficulties of systems integration, in such circumstances Licensees will need to ensure they have alternative systems in place.

"Hold Mail" Accounts

166 "Hold Mail" accounts are accounts where the accountholder has instructed the Licensee not to issue any correspondence to the accountholder's address. Although this is not necessarily a suspicious act in itself, such accounts do carry additional risk to Licensees, and they should exercise due caution as a result.

167 Regardless of the source of "Hold Mail" business, it is recommended on a best practice basis that evidence of identity of the accountholder should be obtained by the Licensee, even where the client was introduced by an Eligible Introducer. "Hold Mail" accounts should be regularly monitored and reviewed.

168 It is recommended that Licensees have controls in place for when existing accounts change status to "Hold Mail", and that the necessary steps to obtain the identity of the account holder are taken where such evidence is not already on the Licensee’s file.

169 Accounts with a "c/o" address should not be treated as "Hold Mail" accounts, as mail is being issued, albeit not necessarily to the accountholder's address. There are of course many genuinely innocent circumstances where a "c/o" address is used, but Licensees should monitor such accounts more closely as they represent a higher risk.

170 Licensees should incorporate procedures to check the current permanent address of hold mail customers wherever the opportunity arises.

Electronic Payment And Message Systems

171 Licensees, must ensure that they keep and maintain records of all payment messages sent via electronic payment and message systems such as SWIFT, in accordance with the provisions of Regulation 8 of the FTRR.

172 Licensees should ideally have effective procedures in place to identify wire transfers lacking appropriate information.

VI - RECORD KEEPING

173 Sections 23, 24 and 25 of the Financial Transactions Reporting Act, 2000 require financial institutions to retain records concerning customer identification and transactions for use as evidence in any investigation into money laundering. This is an essential constituent of the audit trail procedures that the Financial Transactions Reporting Regulations, 2000 seek to establish. If the Financial Intelligence Unit and law enforcement agencies investigating a money laundering case cannot link criminal funds passing through the financial system with the original criminal money generating such funds, then confiscation of the criminal funds cannot be effected. Often the only valid role a financial institution can play in a money laundering investigation is through the provision of relevant records, particularly where the money launderer has used a complex web of transactions specifically for the purpose of confusing the audit trail.

174 The records prepared and maintained by any financial institution on its customer relationships and transactions should be such that:

- requirements of legislation are fully met;
- competent third parties will be able to assess the institution's observance of money laundering policies and procedures;
- any transactions effected via the institution can be reconstructed; and,
- the institution can satisfy court orders or enquiries from the appropriate authorities.

175 The most important single feature of the Financial Transactions Reporting Act, 2000 in relation to record keeping is that it requires relevant records to be retained for at least five years from the date a person ceases to be a facility holder or from the date of completion of a transaction.

Documents Verifying Evidence Of Identity

176 Section 24 of the Financial Transactions Reporting Act, 2000 provides that where a financial institution is required by sections 6, 7, 8, 9, or 11 of the Financial Transactions Reporting Act, 2000 to verify the identity of any person, the financial institution shall keep such records as are

reasonably necessary to enable the nature of the evidence used for the purposes of that verification to be readily identified by the Financial Intelligence Unit.

VII - THE ROLE OF THE MONEY LAUNDERING REPORTING OFFICER

177 The type of person appointed as Money Laundering Reporting Officer will depend upon the size of the bank or trust company and the nature of its business, but he or she should be sufficiently senior to command the necessary authority. Larger banks and trust companies may choose to appoint a senior member of their compliance, internal audit or fraud departments. In small organisations, it may be appropriate to designate the Chief Executive. When several subsidiaries operate closely together within a group, there is much to be said for designating a single Money Laundering Reporting Officer at group level.

178 The Money Laundering Reporting Officer has significant responsibilities. He or she is required to determine whether the information or other matters contained in the transaction report he or she has received gives rise to a knowledge or suspicion that a customer is engaged in money laundering.

179 In making this judgment, he or she should consider all other relevant information available within the bank or trust company concerning the person or business to whom the initial report relates. This may include a review of other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship, and reference to identification records held. If, after completing this review, he or she decides that the initial report gives rise to a knowledge or suspicion of money laundering, then he or she must disclose this information to the Financial Intelligence Unit.

180 The "determination" by the Money Laundering Reporting Officer implies a process with at least some formality attached to it, however minimal that formality might be. It does not necessarily imply that he or she must give his or her reasons for negating, and therefore not reporting any particular matter, but it clearly would be prudent, for his or her own protection, for internal procedures to require that only written reports are submitted to him or her and that he or she should record his or her determination in writing, and the underlying reasons therefor.

181 The Money Laundering Reporting Officer will be expected to act honestly and reasonably and to make his or her determinations in good faith.

Reporting Procedures

182 The national reception point for disclosure of suspicious transaction reports is the Financial Intelligence Unit, 3rd Floor Norfolk House, Frederick Street, P.O. Box SB-50086, Nassau, The Bahamas, Telephone No. (242) 356-9808 or (242) 356-6327, Fax No. (242) 322-5551.

Banks and trust companies should ensure that all contact between their departments or branches with the Financial Intelligence Unit and law enforcement agencies is reported to the Money Laundering Reporting Officer so that an informed overview of the situation can be maintained. In addition, the Financial Intelligence Unit will continue to provide information on request to a disclosing institution in order to establish the current status of a specific investigation.

VIII - EDUCATION AND TRAINING

Requirements

183 Banks and trust companies must take appropriate measures to make employees aware of:

- policies and procedures put in place to detect and prevent money laundering including those for identification, record keeping and internal reporting; and
- the relevant legislation pertaining to money laundering,

and to provide relevant employees with training in the recognition and handling of suspicious transactions.

184 These Guidelines set out what steps banks and trust companies should take to fulfill this requirement.

The Need For Staff Awareness

185 The effectiveness of the procedures and recommendations contained in these Guidelines depend on the extent to which staff of financial institutions appreciate the serious nature of the background against which these Guidelines have been issued. Staff must be aware of their own personal statutory obligations and that they can be personally liable for failure to report information in accordance with internal procedures. All staff should be encouraged to co-operate fully and to provide a prompt report of any suspicious transactions without fear of reprisal.

186 It is, therefore, important that organisations conducting banking and trust activities covered by these Guidelines introduce comprehensive measures to ensure that staff are fully aware of their responsibilities.

Education And Training Programmes

187 Timing and content of training for various sectors of staff will need to be adapted by individual institutions for their own needs. The Financial Intelligence (Transactions Reporting) Regulations, 2000 provide that, at least once per year, financial institutions shall provide relevant employees with appropriate training in the recognition and handling of

transactions carried out by persons who may be engaged in money laundering. The following is recommended:

(a) New Employees

A general appreciation of the background to money laundering, and the subsequent need for reporting of any suspicious transactions to the Money Laundering Reporting Officer should be provided to all new employees who will be dealing with customers or their transactions, irrespective of the level of seniority, within the first month of their employment. They should be made aware of the importance placed on the reporting of suspicions by the organisation, that there is a legal requirement to report, and that there is a personal statutory obligation in this respect. They should also be provided with a copy of the written policies and procedures in place in the financial institution for the reporting of suspicious transactions.

(b) Cashiers/Foreign Exchange Operators/Advisory Staff

Members of staff who are dealing directly with the public are the first point of contact with potential money launderers and their efforts are therefore vital to the organisation's reporting system for such transactions. Training should be provided on factors that may give rise to suspicions and on the procedures to be adopted when a transaction is deemed to be suspicious.

All front line staff should be made aware of the business policy for dealing with occasional customers, particularly where large cash transactions, money transfers, negotiable instruments, certificates of deposit or letters of credit and other guarantees, etc. are involved, and of the need for extra vigilance in these cases.

Branch staff should be trained to recognise that criminal money may not only be paid in or drawn out across branch counters and should be encouraged to take note of credit and debit transactions from other sources, e.g., credit transfers, wire transfers and ATM transactions.

(c) Account/Facility Opening Personnel

Those members of staff responsible for account/facility opening and acceptance of new customers must receive the basic training

given to cashiers or tellers in the above paragraph. In addition, further training should be provided in respect of the need to verify a customer's identity and on the business' own account opening and customer/client verification procedures. They should also be familiarised with the business' suspicious transaction reporting procedures.

(d) Administration/Operations Supervisors and Managers

A higher level of instruction covering all aspects of money laundering procedures should be provided to those with the responsibility for supervising or managing staff. This will include the offences and penalties arising from the Proceeds of Crime Act, 2000 and the Financial Transactions Reporting Act, 2000 for non-reporting and for assisting money launderers; procedures relating to the service of production and restraint orders; internal reporting procedures; and, the requirements for verification of identity, the retention of records, and disclosure of suspicious transaction reports under the Financial Intelligence Unit Act, 2000.

(e) Money Laundering Reporting Officer/or Compliance Officer

In-depth training concerning all aspects of the legislation and internal policies will be required for the Money Laundering Reporting Officer/Compliance Officer. In addition, the Money Laundering Reporting Officer/Compliance Officer will require extensive initial and on-going instruction on the validation, investigation and reporting of suspicious transactions and on the feedback arrangements and on new trends and patterns of criminal activity.

188 It will also be necessary to make arrangements for refresher training at least annually to ensure that staff do not forget their responsibilities.

APPENDIX A

SUMMARY OF EXISTING BAHAMIAN LAW

The existing law pertaining to money laundering and the requirements that financial institutions know their customers are found substantially in the Proceeds of Crime Act, 2000 (Act No. 44 of 2000), the Financial Transactions Reporting Act, 2000 (Act No. 40 of 2000), the Financial Transactions Reporting (Amendment) Act 2001 (Act No. 17 of 2001) the Financial Transactions Reporting Regulations, 2000 (Statutory Instrument No. 111 of 2000), the Financial Transactions Reporting (Amendment) Regulations, 2001 (Statutory Instrument No. 113 of 2001), the Financial Intelligence Unit Act, 2000 (Act No. 39 of 2000), the Financial Intelligence Unit (Amendment) Act, 2001 (Act No. 20 of 2001) and the Financial Intelligence (Transactions Reporting) Regulations, 2001 (Statutory Instrument No. 7 of 2001).

I PROCEEDS OF CRIME ACT, 2000

Confiscation Orders

Section 9 of the Act provides that any person convicted of one or more drug trafficking offences committed after the commencement of this Act shall be liable to have a confiscation order made against him relating to the proceeds of drug trafficking.

For the purposes of this Act a person has benefited from drug trafficking if that person, at any time after the commencement of the Act or for the period of six years prior to proceedings being instituted against him, received any payment or other reward in connection with drug trafficking carried on by him or another person.

Section 10 of the Act allows for a confiscation order to be made against any person convicted for one or more relevant offences committed after the coming into operation of the Act. The "relevant offences" are those offences described in the Schedule to the Act as follows:

(1) An offence under the Prevention of Bribery Act, Chapter 81 of the Statute Laws of The Bahamas, 1987 Edition;

(2) An offence under section 40, 41, or 42 of this Act (Money Laundering);

(3) An offence which may be tried on information in The Bahamas other than a drug trafficking offence;

[4] An offence committed anywhere that if it had occurred in The Bahamas, would constitute an offence in The Bahamas as set out in the Schedule to the Act.

The court must first determine whether such a person has benefited from the principal offence or offences for which he is to be sentenced and secondly from any relevant offences which the court will be taking into consideration in determining his sentence for the principal offence.

For the purposes of the Act, a person benefits from a relevant offence if:

(a) he obtains property as a result of or in connection with its commission and his benefit is the value of such property; and,

(b) he derives a pecuniary advantage as a result of or in connection with its commission and his benefit is the amount of or the value of the pecuniary advantage of an offence. In these circumstances, he is to be treated as if he had obtained instead a sum of money equal to the value of the pecuniary advantage.

Section 11 of the Act provides that for the purpose of determining whether a person has benefited from drug trafficking and for determining the value of his proceeds of drug trafficking the court must assume, unless the contrary is shown:

(a) that any property shown to the court –

(i) to have been held by the defendant; or,
[ii] to have been transferred to him at any time since the beginning of the period of six years ending when the proceeding was instituted against him;

and received by him as a payment or reward in connection with drug trafficking carried on by him;

(b) that any expenditure of his since the beginning of that period was met out of payments received by him in connection with drug trafficking carried on by him;

(c) that, for the purpose of valuing any property received or assumed to have been received by him at any time as such a reward, he received the property free of other interests in it.

Section 15 of the Act provides that a third party who has an interest in any property that is the subject of a confiscation order may apply to the court for an order either before the order is made or otherwise with the leave of the court, declaring the nature, extent and value of his interest.

Charging Orders

Section 27 of the Act provides that a court may make a charging order imposing a charge on property specified in the order for securing the payment of money to the Crown. An application for a charging order may be made only by the Police or the Attorney-General. Property which may be the subject of a charging order includes, inter alia, any monies held by or deposited with a bank or other financial institution, the stock of any body corporate, and a debt instrument.

Production Orders

Section 35 of the Act empowers a Stipendiary and Circuit Magistrate upon application by a Police officer of or above the rank of Inspector, to make a production order where the Magistrate is satisfied that there is reasonable cause to believe that any person is in possession of material in respect of which a drug trafficking offence or relevant offence has been committed. The order would require a person to produce relevant material in his possession for the Police.

A production order shall not extend to items subject to legal privilege. However, it shall have effect notwithstanding any obligation as to confidentiality or other restriction upon the disclosure of information imposed by the Banks and Trust Companies Regulation Act, 2000, the Central Bank of The Bahamas Act, 2000, any other statute or otherwise and shall not give rise to any civil liability. Where a production order requires information which is restricted under the Banks and Trust Companies Regulation Act, 2000 or the Central Bank of The Bahamas Act, 2000, application for an order shall be made ex-parte to a judge in chambers.

A production order may be made in relation to material in the possession of a Government Department (excluding the Financial Intelligence Unit).

Monitoring Order

Section 39 of the Act provides that a police officer may apply to a Judge in Chambers for a monitoring order directed to any police officer of or above the rank of Inspector, directing a bank or trust company to give the officer information obtained by the institution in respect of transactions conducted through an account or accounts held by a person under investigation, with the institution.

The monitoring order is to be made where the Judge is satisfied by evidence on oath that there is reasonable cause to believe that a person has committed or is about to commit a drug trafficking offence or a relevant offence; or was involved in the commission or is about to become involved in the commission of such an offence; or has benefited directly or indirectly from the commission of such an offence. The disclosure of information in these circumstances is not to be treated as a breach of any restriction upon disclosure of information imposed by the Banks and Trust Companies Regulation Act, 2000, The Central Bank of The Bahamas Act, 2000, any other statute or otherwise. Additionally, such disclosure shall not give rise to any civil liability.

The Offence of Money Laundering

Section 40 of the Act provides that a person is guilty of the offence of money laundering if he uses, transfers, sends or delivers to any person or place any property which, in whole or in part directly or indirectly represents proceeds of criminal conduct; or disposes of, converts, alters or otherwise deals with that property in any manner and by any means with the intent to conceal or disguise such property.

A person is also guilty of money laundering if he knows, suspects or has reasonable grounds to suspect that any property in whole or in part directly or indirectly represents another person's proceeds of criminal conduct and he uses, transfers, sends or delivers to any person or place that property; or disposes of or otherwise deals with in any manner by any means that property, with the intent to conceal or disguise the property.

Section 41 of the Act provides inter alia that it is an offence for a person to assist another to retain or live off the proceeds of criminal conduct knowing, suspecting, or having reasonable grounds to suspect that the other person is or has been engaged in or has benefited from criminal conduct.

It is a defence for a person to prove that he or she did not know, suspect or have reasonable grounds to suspect that -

(a) the arrangement in question related to any person's proceeds of criminal conduct; or,

(b) the arrangement facilitated the retention or control of any property by or on behalf of the suspected person; or,

(c) by arrangement any property was used as mentioned in section 41(1)(b).

Further, it is a defence for a person to prove that he intended to disclose to a police officer a suspicion, belief or matter that any funds or property are derived from or used in connection with criminal conduct; but there is a reasonable excuse for failing to do so as prescribed in subsection (2)(b) of the Act.

Section 42 of the Act provides that a person is guilty of an offence if he knows, suspects or has reasonable grounds to suspect that any property in whole or in part directly or indirectly represents, another person's proceeds of criminal conduct, and he acquires or uses that property or has possession of it.

It is a defence for a person to prove that he acquired or used the property or had possession of it for adequate consideration.

Penalty for failing to disclose suspicious transaction

Section 43 of the Act makes it an offence for a person who knows suspects or has reasonable grounds to suspect that another person is engaged in money laundering, which relates to any proceeds of drug trafficking or any relevant offence, to fail to disclose this to the Financial Intelligence Unit or to a police officer.

A person is also guilty of an offence where the information, or other matter, on which his knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment and he fails to disclose the information or other matter to a police officer as soon as is reasonably practicable after it comes to his attention.

It is a defence to prove that the person had a reasonable excuse for not disclosing the information or other matter in question. It should be noted that

a person is not required to disclose information or to provide a document which is subject to legal professional privilege. However, a counsel and attorney-at-law may be required to provide the name and address of his client or principal.

Offence of disclosing information prejudicial to an investigation ("Tipping Off")

Section 44 of the Act makes it an offence to disclose information that is likely to prejudice an investigation if the person knows, suspects or has reasonable grounds to suspect that an investigation into money laundering is being, or is about to be, conducted or if he knows, suspects or has reasonable grounds for suspecting that a disclosure has been made under section 41, 42 or 43.

It is a defence to prove that the person did not know or suspect that the disclosure was likely to prejudice the investigation or that he had lawful authority or reasonable excuse for making the disclosure.

Penalty for offences under sections 43 and 44

A person guilty of an offence under section 43 to 44 shall be liable on summary conviction, to imprisonment for three years or to a fine of $50,000.00 or both; or on conviction on information, to imprisonment for ten years or an unlimited fine or both.

Penalty for money laundering

Section 45 of the Act provides that a person guilty of an offence under section 40, 41 or 42 shall be liable on summary conviction to imprisonment for five years or a fine of $100,000.00 or both; and on conviction on information, to imprisonment for twenty years or an unlimited fine or both.

External Confiscation Orders

Section 49 of the Act provides that the Minister responsible for the Police may, by order direct in relation to a country outside The Bahamas, designated by the order, that subject to such modifications as may be specified, the Act shall apply to external confiscation orders and to proceedings which have been or are

to be instituted in the designated country and may result in an external confiscation order being made there.

Section 50 of the Act provides that upon the application made by or on behalf of the government of a country designated by an Order of the Minister under section 49, the Supreme Court may register an external confiscation order made in a designated country, if satisfied of certain conditions, and such registered order shall be enforceable in The Bahamas in the same manner as a confiscation order made by a court in The Bahamas. (Countries have been designated by Statutory Instrument No. 6 of 2001, which includes most of the major countries).

Offences by a body corporate

Section 54 of the Act provides that where a body corporate is found guilty of an offence under this Act and the offence is proven to have been committed with the consent or connivance of any director, manager, secretary or other similar officer of the body corporate or any person who was purporting to act in any such capacity he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

II. THE FINANCIAL TRANSACTIONS REPORTING (AMENDMENT) ACT, 2003

The Financial Transaction Reporting (Amendment) Act, 2003, ("the Act") mandates that financial institutions as defined in section 3 of the Act, verify the identity of their customers in the circumstances set out in the Act.

Section 2(3) of the Act restricts the definition of "financial institution" to include only five of the institutions listed in section 3 of the Act, namely, banks or trust companies, companies carrying on life assurance business; licensed casino operators; broker dealers, and investment fund administrators or operators of investment funds (see section 3(1)(a), (b), (e), (f) and (i)). The occasions when a Licensee may obtain and rely upon written confirmation of identity from another financial institution are set out in Part IV of these Guidelines in paragraph 147 and 148 above.

Section 3 of the Act defines "Financial Institution".

The Act makes it mandatory for financial institutions to verify the identity of the following persons:

Persons who wish to become facility holders

Section 6 of the Act provides that the identity of such persons must be verified before they become facility holders (see section 6(1) and 6(2)).

Existing facility holders whose identities are doubtful

Where during the course of a business relationship the financial institution has reason to doubt the identity of an existing facility holder, the financial institution shall seek to verify the identity of such facility holder (see section 6(4)).

Each and every existing facility holder

The identity of any customer having a facility established prior of 29th December 2000 must be verified by the 1st April 2004.

Where the identity of such a customer remains unverified as of the 1st April 2004, licensees must notify the Central Bank who shall issue written directions to licensees with respect to unverified facilities. Such directions shall include the power to suspend or discontinue any further activity in relation to the facility of such a customer until verification has taken place (see section 6(6)).

Occasional Transactions

Section 7 of the Act provides for the mandatory verification by a financial institution of the identity of the following persons:
A person who conducts an occasional transaction by, through or with a financial institution in any case where:

(a) the amount of cash involved in the transaction exceed the prescribed amount of $15,000.00 (this verification must take place before the transaction is conducted) and in these circumstances, the financial institution shall also ask the person who is conducting or who has conducted the transaction whether or not the transaction is or was being

conducted on behalf of any other person (see section 7(1)(a), 7(4)(a) and 7(5)); or

(b) one or more other occasional transactions have been or are being conducted by that person or any other person through the financial institution;

(c) the financial institution has reasonable grounds to believe that the transactions have been or are being structured so that the amount of cash involved in the transaction do not exceed the prescribed amount of $15,000.00; and

(d) the total amount of cash involved in those transactions exceeds the prescribed amount (see section 7(1)(b)).

In determining whether or not any transactions are or have been structured to avoid the application of section 7(1)(a), the financial institution shall consider the following factors:

(a) the time frame within which the transactions are conducted;

and

(b) whether or not the parties to the transactions are the same person, or are associated in any way (see section 7(3)).

In any case where the conditions referred to in (b), (c) or (d) above apply, verification must be made as soon as practicable after the conditions specified in section 7(1)(b) are satisfied in respect of that transaction (see section 7(4)(b)).

Section 8 of the Act provides for the mandatory verification by a financial institution of the identity of the following persons:

A person on whose behalf an occasional transaction is being conducted by, through or with a financial institution in circumstances where the cash involved in the transaction exceed the prescribed amount and the financial institution has reasonable grounds to believe that the person conducting the transaction does so on behalf of any other person or persons. Such verification must take place before the transaction is completed (see section 8(1) and 8(4)).

A person on whose behalf an occasional transaction has been conducted, in circumstances where the financial institution has reasonable

grounds to believe, after the occasional transaction has been conducted, that the person who conducted the transaction was acting on behalf of another person or persons.

A person of whom it is believed that one or more occasional transactions are or have been conducted on his behalf in circumstances where the transactions have been or are being structured to avoid the application of section 8(1) and the total amount of cash involved in those transactions exceed the prescribed amount (see section 8(2)).

In determining whether or not any transactions are or have been structured to avoid the application of section 8(1), the financial institution shall consider the following factors:

(a) the time frame within which the transactions are conducted; and,

(b) whether or not the parties to the transactions are the same person(s), or are associated in any way (see section 8(3)).

Section 9 of the Act provides for the mandatory verification of the identity of the persons on whose behalf a transaction is being or has been conducted by a facility holder through a facility provided by a financial institution where:

- **in the case of a single transaction**

  (a) the amount of cash involved in the transaction exceed the prescribed amount of $15,000.00; and,

  (b) the financial institution has reasonable grounds to believe that the person is conducting the transaction on behalf of others.

  Such verification must take place before the transaction is conducted (see section 9(1) and 9(4)).

- **in the case where the facility holder has also conducted or is conducting one or more other transactions through that facility**

  (a) the financial institution has reasonable grounds to believe that the facility holder is conducting the transaction on behalf of others;

(b) the financial institution has reasonable grounds to believe that the transactions have been structured to avoid the application of the mandatory verification procedure required by the Act; and

(c) the total amount of cash involved in the transactions exceed the prescribed amount.

Such verification must take place as soon as practicable after these conditions are satisfied (see section 9(2) and 9(5)).

In determining whether or not any transactions are or have been structured to avoid the application of section 9(1), the financial institution shall consider the following factors -

(a) the time frame within which the transactions are conducted;

(b) whether or not the parties to the transactions are the same person(s) or are associated in any way (see section 9(3)).

Section 10A of the Act provides for the mandatory verification by a financial institution to verify the identity of any person (whether as a facility holder or not) where they know, suspect or have reasonable grounds to suspect is conducting or proposes to conduct a transaction which involves the proceeds or criminal conduct as defined in the Proceeds of Crime Act, 2000 or is an attempt to avoid the enforcement of the Proceeds of Crime Act, 2000.

Section 11 of the Act provides that where verification of identity is required by the Act, it shall be done by means of such documentary or other evidence as is reasonably capable of establishing the identity of a person, including official documents and structural information in the case of corporate entities.

A financial institution may rely in whole or in part on evidence used by it on an earlier occasion to verify that person's identity, if the institution has reasonable grounds to believe that the evidence is still reasonably capable of establishing the identity of that person.

Such verification may be accepted from a foreign financial institution if that institution is located in a country mentioned in the First Schedule.

Section 12 of the Act provides that an offence is committed where a financial institution:

(a) in contravention of section 6(2), permits a person to become a facility holder in relation to any facility without having first verified the identity of that person;

(b) in contravention of section 7(4)(a), permits any person to conduct an occasional transaction in excess of $15,000.00 without first having verified the identity of that person;

(c) in contravention of section 7(4)(b), fails to verify the identity of a person conducting an occasional transaction as soon as practicable after the conditions set out in section 7(1)(b) have been satisfied in respect of that transaction;

(d) in contravention of section 8(4) fails to verify the identity of a person on whose behalf an occasional transaction in excess of $15,000.00 is being or has been conducted;

(e) in contravention of section 8(5), fails to undertake the verification required by section 8(2) in relation to persons conducting an occasional transaction in excess of 15,000.00 in circumstances where it reasonably appears that the transaction is being conducted on behalf of any other person or persons and that the transactions are or have been structured to avoid verification of identity;

(f) in contravention of section 9(4), fails, before a transaction is conducted, to verify the identity of a person on whose behalf a facility holder is conducting a transaction in excess of $15,000.00 that where it has reasonable grounds to believe the circumstances set out in section 9(1) exist, and;

(g) in contravention of section 9(5), fails to undertake the verification required by section 9(2);

A financial institution which commits any of the foregoing offences is liable on summary conviction to a fine not exceeding:

(a) in the case of an individual, $20,000.00;

(b) in the case of a body corporate, $100,000.00.

Suspicious Transactions

Section 14 of the Act makes it mandatory for a financial institution to report to the Financial Intelligence Unit any transaction conducted by, through or with a financial institution or any proposed transaction (whether or not the transaction involves funds) where the financial institution knows, suspects or has reasonable grounds to suspect that the transaction or proposed transaction involves proceeds of criminal conduct as defined in the Proceeds of Crime Act, 2000, or any offence under the Proceeds of Crime Act, 2000, or an attempt to avoid the enforcement of any provision of the Proceeds of Crime Act, 2000.

The financial institution must as soon as practicable after forming a suspicion, report the transaction to the Financial Intelligence Unit.

Every suspicious transaction report shall be in writing, and shall contain the details set out in the Second Schedule to the Act.

A report must also contain the grounds on which the financial institution holds a suspicion.

A report may be forwarded to the Financial Intelligence Unit by way of facsimile transmission, or by other means (including without limitation, electronic mail or other similar means of communication) as may be agreed from time to time between the Financial Intelligence Unit and the financial institution concerned.

Oral Reports

Section 14 of the Act also provides that where the urgency of the situation so requires, a suspicious transaction report may be made orally to the Financial Intelligence Unit; however, the financial institution shall, as soon as practicable, forward to the Financial Intelligence Unit a suspicious transaction report that complies with the requirements of the Act.

Penalty for failing to report suspicious transactions

A person who contravenes the provisions of section 14(1) shall be liable on summary conviction to a fine not exceeding – in the case of an individual, $20,000.00 and, in the case of a body corporate, $100,000.00 (see section 20(2)).

It is a defence for a person to prove that he took all reasonable steps to ensure that he complied with the provisions of section 14(1) or that, in the circumstances of the particular case, he could not reasonably have been expected to ensure that he complied with the provision (see section 21).

Auditors to report suspicious transactions

Section 15 of the Act provides that an auditor is under a duty to report suspicious transactions to any member of the Police, where in the course of carrying out the duties of his occupation as an auditor, he has reasonable grounds to suspect, in relation to any transaction that the transaction is or may be relevant to the Proceeds of Crime Act, 2000. No civil, criminal or disciplinary proceedings shall lie against an auditor who makes a suspicious transaction report pursuant to section 15.

Protection of persons reporting suspicious transactions

Section 16 of the Act provides protection from civil, criminal or disciplinary proceedings to persons who report suspicious transactions in accordance with the provisions of the Act.

Legal Professional Privilege

Section 17 of the Act provides that the mandatory reporting provisions of the Act do not apply to the disclosure of privileged information by a Counsel and Attorney, except however, that where the information consists wholly or partly of, or relates wholly or partly to, the receipts, payments, income, expenditure or financial transactions of a specified person (whether a counsel and attorney, his or her client or any other person), the information shall not be a privileged communication if it is contained in or comprises the whole or part of any book,

account, statement or other record prepared or kept by the counsel and attorney in connection with a client's account of the counsel and attorney.

Persons to whom suspicious transaction reports may be disclosed

Section 18 of the Act restricts the persons to whom a financial institution may disclose that they have made or are contemplating making a suspicious transaction report. Apart from the Financial Intelligence Unit, reports may be disclosed only to the financial institution's supervisory authority; the Commissioner of Police or a member of the Police authorized by the Commissioner to receive the information; an officer or employee or agent of the financial institution, for any purpose connected with that person's duties; a counsel and attorney for the purpose of obtaining legal advice or representation in relation to the matter; and, the Central Bank of The Bahamas for the purpose of assisting the Central Bank of The Bahamas to carry out its function under the Central Bank of The Bahamas Act, 2000.

Section 20(7) of the Act provides that a person who knowingly contravenes section 18(1) to (3) is liable upon summary conviction to:

(1) in the case of an individual, a fine not exceeding $5,000.00 or to imprisonment for a term not exceeding 6 months;

(2) in the case of body corporate, a fine not exceeding $20,000.00.

Protection of Identity

Section 19 of the Act provides inter alia that no person shall be required to disclose, in any judicial proceeding, any suspicious transaction report, or any information the disclosure of which will identify, or is reasonably likely to identify, the officer, employee or agent of a financial institution who has handled a transaction in respect of which a suspicious transaction report was made, or who has prepared a suspicious transaction report, or who has made a suspicious transaction report, unless the Judge or, as the case requires, the person presiding at the proceeding is satisfied that the disclosure of the information is necessary in the interests of justice.

Penalty for making false statements and for "Tipping Off"

Section 20 of the Act provides that:

(1) it is an offence for a person, in making a suspicious transaction report, to make a statement which they know to be false or misleading in a material particular or to omit from any statement any matter or thing without which the person knows that the statement is false or misleading in a material particular. A person who commits this offence is liable on information to a fine not exceeding $10,000.00 (see section 20(3));

(2) a person who contravenes sections 18(1) to (3), for the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for that person or any other person, or with intent to prejudice any investigation into the commission or possible commission of a money laundering offence, commits an offence and is liable on summary conviction to a term of imprisonment not exceeding two years (see section 20(4));

(3) an officer, employee or agent of a financial institution who, having become aware, in the course of that person's duties as such an officer or employee or agent, that any investigation into any transaction or proposed transaction that is the subject of a suspicious transaction report is being, or may be, conducted by the Police:

(a) knowing that he or she is not legally authorised to disclose the information; and,
(b) either:
(i) for the purpose of obtaining, directly or indirectly, an advantage or a pecuniary gain for that person or any other person; or,

(ii) with intent to prejudice any investigation into the commission or possible commission of a money laundering offence;

discloses that information to any other person is guilty of an offence (see section 20(5)).

Penalty

Summary conviction for these offences carries a term of imprisonment not exceeding two years.

Application of information contained in a suspicious transaction report

Section 22 of the Act provides that information contained in a suspicious transaction report is deemed to be obtained for certain limited purposes such as, inter alia: the detection, investigation, and prosecution of offences against the Act; the enforcement of the Proceeds of Crime Act, 2000; or, the detection, investigation and prosecution of any relevant offence (within the meaning of the Proceeds of Crime Act, 2000), in any case where that offence may reasonably give rise to, or form the basis of, any proceedings under the Proceeds of Crime Act, 2000.

Retention of Records

Section 23 of the Act provides that financial institutions are obligated to retain transaction records for a period of not less than five years after the completion of a transaction. The records that are to be retained are those that are reasonably necessary to enable the Financial Intelligence Unit to re-construct a transaction.

The records should include information concerning the nature of the transaction; the amount of the transaction, and the currency in which it was denominated; the date on which the transaction was conducted; the parties to the transaction; and, where applicable, each facility (whether or not provided by the financial institution) directly involved in the transaction.

Section 24 of the Act provides that where a financial institution is required by section 6, 7, 8, 9, or 11 of the Act, to verify the identity of any person, the financial institution must keep such records as are reasonably necessary to enable the nature of the evidence used for the purposes of that verification to be readily identified by the Financial Intelligence Unit (see section 24(1)).

The obligation to retain records also applies where a financial institution verifies the identity of any person by confirming the existence of a facility provided by another financial institution. In this instance, the records that are retained should be such as are reasonably necessary to enable the Financial Intelligence Unit to readily identify, at any time, the identity of the other financial

institution, the identity of the relevant facility and the identity confirmation of the person (see section 24(3)).

Such reports may comprise a copy of the evidence so used or, where it is not practicable to retain that evidence, such information as is reasonable necessary to enable that evidence to be obtained.

Records relating to the verification of the identity of persons making a request to become facility holders, and to the identity of existing facility holders must be retained for five years after a person ceases to be a facility holder (see section 24(4)).

Records relating to the verification of the identity of any non-facility holder in relation to a facility, where the verification was carried out pursuant to section 9, with respect to a person who is such a facility holder, shall be kept by a financial institution for a period of not less than five years.

In relation to any other person, records relating to the verification of the identity of any person shall be kept for a period of not less than five years after the verification was carried out.

Section 25 of the Act directs financial institutions to keep records which are prescribed by any regulations made under this Act, pursuant to section 42, and to retain them for any prescribed period.

Section 26 of the Act provides that records must be kept either in written form in the English language or so as to enable the records to be readily accessible and readily convertible into written form in the English language.

Section 27 of the Act provides that a company need not retain records where a company has been liquidated and finally dissolved; or, where a partnership has been dissolved.

Section 28 of the Act provides that a financial institution shall ensure the destruction of records retained for the purposes of Part IV of the Act, as soon as practicable after the expiry of any retention period provided by Part IV of the Act.

Destruction of records is not required where there is a lawful reason for retaining them.

There is a lawful reason for retaining a record if the retention of a record is necessary:

(a) in order to comply with the requirements of any other written law;

(b) to enable any financial institution to carry on its business; or

(c) for the purposes of the detection, investigation or prosecution of any offence.

Section 29 of the Act provides that other laws which require any financial institution to keep or retain any record, are not affected by Part IV of the Act.

Section 30 of the Act provides that it is an offence for a financial institution to fail, without reasonable excuse, to retain or properly keep records sufficient to satisfy the requirements of this section.

A person guilty of an offence under this section is liable on summary conviction to a fine not exceeding in the case of an individual, $20,000.00 and in the case of a body corporate, $100,000.00

III FINANCIAL TRANSACTIONS REPORTING (AMENDMENT) REGULATIONS, 2003

These Regulations prescribe the information which a financial institution is required to obtain to verify the identity of any person.

Regulation 2 provides that for the purposes of Part II of the Financial Transactions Reporting (Amendment) Act, 2003, the prescribed amount shall be the sum of $15,000.00.

Regulation 3 sets out the information that financical institutions must obtain when they seek to verify the identity of individual customers namely the full and correct name of the individual, their address, date and place of birth, and the purpose of the account (facility) and the nature of the business relationship. In addition, regulation 3 introduces a risk based approach to customer due

diligence and provides financial institutions with guidance on the type of information and documentation they may rely upon (apart from the required information) when verifying an individual customer's identity and includes information such as the source of funds, telephone and fax numbers(if any), occupation and name of employer (if self employed, the nature of the self employment), copy of the relevant pages of passport, drivers licence, voter's card, national identity card or such other identification document bearing a photographic likeness of the person as is reasonably capable of establishing the identity of the person, or such documentary or other evidence as is reasonably capable of establishing the identity of that individual.

Regulations 4 and 5 adopt a risk based approach to verifying the identities of corporate entities, whether incorporated in The Bahamas or elsewhere (Regulation 4), partnerships and other unincorporated businesses (Regulation 5) and provides financial institutions with guidance on the type of information and documentation they may rely upon when verifying these entities.

Regualtion 5A provides for exemption from verification procedures by those customers with a Bahamian dollar facility of or below $15,000.00 and certain financial institutions and other agencies or bodies.

Regulation 7 provides that where any request is made to a financial institution, by telephone, internet, or written communication for a person, corporate entity or partnership to become a facility holder, the financial institution should (subject to certain exceptions) obtain the information set out in regulation 3 to 5 as appropriate.

Regulation 7A requires financial institutions to verify the identities of the beneficial owners of all facilities. In the case of corporate entities the obligation to verify beneficial owner identity is limited to those beneficial owners having a controlling interest in the corporate entity. For the purposes of these Guidelines, the Central Bank defines "controlling interest" as an interest of ten percent or more of a corporate entity's voting shares.

Regulation 9 requires further verification of customer identity (after the establishment of the business relationship), if there is a material change in the way a customer's facility is operated. Although "material change" is not defined

in the regulation, the Central Bank is of the view that a material change is a change which is inconsistent with a facility holder's account profile. Financial institutions are required to monitor facility holders for consistency with the facility holder's stated account purposes during the business relationship.

Regulation 10 provides that where a facility holder closes one facility and opens another facility, the financial institution shall confirm the identity of the facility holder and obtain any additional information with respect to the facility holder and all records relating to the existing account shall be transfered to the new facility and retained for the relevant period.

Regulation 11 provides that records required by section 23, 24, or 25 of the Act to be kept by any financial institution may be stored on microfiche, computer disk or in other electronic form.

IV FINANCIAL INTELLIGENCE UNIT ACT, 2000

By virtue of section 3, the Financial Intelligence Unit Act, 2000 (No. 39 of 2000) ("the Act") establishes the Financial Intelligence Unit of The Bahamas (the "FIU") giving it wide powers to enter into contracts and to do all such things necessary for the purpose of its functions.

Section 4(1) of the Act empowers the FIU to act as the agency responsible for receiving, analysing, obtaining and disseminating information which relates or may relate to the proceeds of offences under the Proceeds of Crime Act, 2000.

Section 4(2)(a)-(i) of the Act provide that the FIU may:

- receive all disclosures of information required to be made pursuant to the Proceeds of Crime Act, 2000;
- receive information from any Foreign Financial Intelligence Unit;

- order in writing any person to refrain from completing any transaction up to a maximum period of seventy-two hours;
- freeze a person's bank account for a maximum period of five days upon receipt of a request from a foreign FIU or law enforcement authority including the Commissioner of Police of The Bahamas;
- require the production of information (except information subject to legal professional privilege) which it considers relevant to fulfill its functions;
- share information relating to the commission of an offence under the Proceeds of Crime Act, 2000 with the local law enforcement agency including the Commissioner of Police;
- provide information to foreign FIU's relating to the commission of an offence under the Proceeds of Crime Act, 2000;
- enter into any agreement or arrangement in writing with a foreign FIU for the discharge or performance of the functions of the FIU;
- inform the public and financial and business entities of their obligations under measures that have been or might be taken to detect, prevent and deter the commission of offences under the Proceeds of Crime Act, 2000;
- retain a record of all information it receives for a minimum of five years after the information is received.

Section 4(3) of the Act provides that it is an offence for a person to fail or refuse to provide this information and on summary conviction a person is liable to a fine not exceeding $50,000.00 or to imprisonment for a term not exceeding two years or to both such fine and imprisonment.

Section 6 of the Act provides that no order for the provision of information, documents or evidence may be issued in respect of the FIU or against the Minister, Director, Officers or personnel of the FIU or any person engaged pursuant to this Act.

Section 7 of the Act provides that no action shall lie against the Minister, Director, Officers or personnel of the FIU or any person acting under the direction of the Director, for anything done or omitted to be done in good faith and in the administration or discharge of any functions, duties or powers under this Act.

No Civil or Criminal Liability

Section 8 of the Act provides that no proceedings for breach of banking or professional confidentiality may be instituted against any person or against directors of a financial or business entity who transmit information or submit reports in good faith in pursuance of this Act or the Proceeds of Crime Act, 2000.

Section 8(2) of the Act further provides that no civil or criminal liability action may be brought nor any professional sanction taken against any person or against directors or employees of a financial or business entity who in good faith transmit information or submit reports to the FIU.

Section 9 of the Act prohibits disclosure of information obatined by any person as a result of his connection with the Financial Intelligence Unit, unless this is required or permitted under this Act or any written law.

Any person who contravenes this provision commits an offence and shall be liable on summary conviction to a fine not exceeding $10,000.00 or to a term of imprisonment not exceeding one year or to both such fine and imprisonment.

V FINANCIAL INTELLIGENCE (TRANSACTIONS REPORTING) REGULATIONS, 2001

The Financial Intelligence (Transactions Reporting) Regulations, 2001 (Statutory Instrument No. 7 of 2001) require financial institutions to establish and maintain the following procedures and practices:

Regulation 3 provides that a financial institution shall establish and maintain identification procedures in compliance with Part II of the Financial Transactions Reporting Act, 2000 and the provisions of the Financial Transactions Reporting Regulations, 2000.

Regulation 4 provides that a financial institution shall establish and maintain record-keeping procedures in compliance with Part IV of the Financial Transactions Reporting Act, 2000 and the provisions of the Financial Transactions Reporting Regulations, 2000.

Regulation 5 provides, inter alia, that a financial institution shall institute and maintain internal reporting procedures which include provision for the appointment of a Money Laundering Reporting Officer and a Compliance Officer. These roles may be performed by the same person.

The Money Laundering Reporting Officer must be registered with the FIU. Financial Institutions must institute and maintain internal reporting procedures which include provisions requiring the Money Laundering Reporting Officer to disclose to the FIU, relevant agency or to a police officer the information or other matter contained in a suspicious transaction report, where the Money Laundering Reporting Officer knows, suspects or has reasonable grounds to suspect a person is engaged in money laundering.

Regulation 6 places an obligation on financial institutions to provide appropriate training from time to time for all relevant employees, at least once per year. Financial Institutions are required to take appropriate measures from time to time to make all relevant employees aware of the provisions of the Financial Intelligence Unit Act, 2000 and the Regulations made thereunder, the Financial Transactions Reporting Act, 2000, the Financial and Corporate Service Providers Act, 2000, the Proceeds of Crime Act, 2000, and any other statutory provision relating to money laundering.

Employees must also be made aware of the procedures maintained by the financial institution in compliance with the duties imposed under these Regulations.

Training must be given to all new relevant employees as soon as practicable after their appointment.

Regulation 8 provides that failure to comply with the requirements of these Regulations is an offcence punishable on summary conviction to a fine of $10,000.00 and on conviction on information to a fine of $50,000.00 for a first offence and to a fine of $100,000.00 for a second or subsequent offence.

It is a defence to prove that a financial institution took all reasonable steps and exercised due dilligence to comply with the requirements of these Regulations.

In determining whether a financial institution has complied with the requirements of these Regulations, the trial court shall take account of any relevant guidelines issued by the FIU or the relevant agency or both.

APPENDIX B

1. IDENTIFICATION PROCEDURES

Information on the status of sanctions can be obtained from websites such as http://www.fco.gov.uk. Other useful websites include: http://www.un.org; http://www.fbi.gov; http://www.ustreas.gov; http://www.bankofengland.co.uk; http://www.osfi-bsif.gc.ca.

2. NON-PROFIT ASSOCIATIONS (INCLUDING CHARITIES)

For a list of all IRS recognized non-profit organizations including charities go to www.guidestar.org; and for a list of registered charities go to www.charity-commission.gov.uk. For various reasons, these bodies will not hold exhaustive lists.

3. POLITICALLY EXPOSED PERSONS ("PEPs")

(a) For information on the assessment of country risks see the Transparency International Corruption Perceptions Index at www.transparency.org.

(b) For information about recent developments in response to PEPs risk, visit the Wolfsberg Group's web site at www.wolfsberg-principles.com. In addition Licensees should be aware of recent guidance from the United States of America on enhanced scrutiny for transactions that may involve the proceeds of foreign official corruption. This can be found on the Internet at www.federalreserve.gov.

APPENDIX C

Anti-Money Laundering Flowchart Summary of Identification Checks

Note: This flow chart is designed as a summary document and may not be exhaustive. Financial Institutions should refer to specific provisions within the legislation and these guidelines to ascertain the full requirements.

DIRECT CUSTOMER FOR BUSINESS